The sys admin's daily grind: tcpflow and HugeURL

Double Feature

First the fun, then the pleasure: This month, we look at a TCP that administrators have to take seriously, followed by some URL fun. *By Charly Kühnast*

If you need to smooth the kinks out of your network services, very likely you will take Tcpdump and Wireshark out of your toolbox. But honestly, both are slightly less than intuitive, and you need to be a genuine expert to interpret the results. Tcpflow [1], on the other hand, is infinitely more intelligible. Instead of presenting the results packet by packet, it collects them as a data stream – thus, the "flow" in the tool's name.

Tcpflow organizes all of your open connections in source-target pairs and gives you a contiguous summary of the data traffic, with no need to worry about sequence numbers and packets out of order. The typical command looks something like:

```
tcpflow -i eth0 -c -e
```

The `-i eth0` parameter selects the interface on which to listen; `-c` directs data on the console.

If you leave out the `-c`, the tool writes the content of each flow to a separate file. The file name is based on the source IP, target IP, and port numbers. The `-e` parameter, which does not seem to be available on some Linux distributions, color-codes the client/server connections on the console. In the style of tcpdump, I can enable filters that restrict the display to specific sources, targets, or ports. The following line

```
tcpflow -i eth0 -c -e port 143
```

only lists the IMAP connections. The screenshot in Figure 1 shows my browser's HTTP connection; I happen to be accessing the German version of *Linux Magazine* online.

This example shows how tcpflow also reveals the content of a cookie sent to me by the website.

Figure 1: Tcpflow collates packet dumps from the client (top left) and the server (bottom left) to create flows. The right-hand image shows one huge URL from HugeURL.com.

The Longer, the Better

About a year ago, I wrote about the URL abbreviator Yourls (Your Own URLs) [2]. Yourls uses Apache's `Mod_rewrite` function to create practical short URLs from long ones. But, you have to consider whether these fast-food URLs are detrimental to our web culture. Thanks to the self-healing properties of our global village, the counterrevolution is already in full swing; irate administrators are fighting back with URLs of epic dimensions. To generate them, surf to HugeURL.com [3], a service that converts a simple web address (*www.linux-magazin.de*) into a monster (Figure 1). ■■■

INFO

[1] tcpflow: *http://www.circlemud.org/~jelson/software/tcpflow/*

[2] "Short Story" by Charly Kühnast, *Linux Magazine* March 2010, pg. 59: *http://www.linux-magazine.com/Issues/2010/112/SHORT-STORY*

[3] HugeURL.com: *http://hugeurl.com*

AUTHOR

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, freshwater aquariums, and learning Japanese, respectively.