Monitoring network traffic with Ruby and Pcap

By *srlinuxx*
Created *06/10/2005 - 9:25am*
Submitted by srlinuxx on Thursday 6th of October 2005 09:25:18 AM Filed under HowTos [1]

There are many situations where the ability to monitor network traffic can save a lot of time and effort. If you want to reverse engineer a network protocol, keep an eye on junior's browsing habits, or blackmail your evil boss, Ruby and libpcap can make it easy! Libpcap is a packet sniffing library originally designed by the Lawrence Berkeley National Laboratory for use with their tcpdump utility. With this excellent Ruby binding for libpcap, you can monitor traffic all over your network with only a few simple lines of code. Let's start with a simple script that will display the URLs of remote files accessed by local network users via web browser.

Full Article [2].

HowTos

Source URL: http://www.tuxmachines.org/node/2925

Links:
[1] http://www.tuxmachines.org/taxonomy/term/98
[2] http://arstechnica.com/columns/linux/linux-20051002.ars