A field guide to TCPDump

What is it? TCPDump is an extremely useful tool to inspect network traffic.

How do I call it? `tcpdump [options] [filter query]`

1. (Most useful) Command-line options

-X	Print the contents of each packet in hex and ascii	-v[v][v]	Turn on verbose output
-i eth0	Only listen on eth0	-n	Don't convert IP addresses to domain names.
-w file.pcap	Write contents of dump to file.pcap. The contents can then be examined with a program like Wireshark.	-F <file>	Read filter expression from <file>
-k NP	Display process name and PID (-only)		

2. Filter language

Filters tell TCPDump which part of the traffic it should display. You can chain filters using the \`and\`, \`or\` and \`not\` operators.

[tcp|udp] port <portnum>	Match all TCP or UDP packets going through <portnum>
[src|dst] host <hostname>	Match all the packets arriving or departing to <hostname>
<filter> and <filter> | <filter> or <filter> | not <filter>	Combine/negate filters

3. Examples

Filter	Explanation	Filter	Explanation
dst host example.com	Capture all packets going to host example.com	tcp and port imap	Capture all IMAP traffic
src host google.com	Capture all packets coming from google.com	portrange 443-447	Capture all traffic on port numbers 443 to 447
dst port 80	Capture all packets going to port 80		

Hastily made by Karim Hamidou – http://khamidou.com/tcpdump