tcpdump cheat sheet

running tcpdump:

	input	optional		
live packet capture * privilege required	-i <interface> use ifconfig to determine	-A	ascii	-w <out_file> -c <num_packets> -F <bpf_filter>
		-X	hex	
		-e	show ethernet header	
analysis of pcap file	-r <pacp_file>	-n	don't resolve ips/ports	
		-v[vv]	increase verbosity	
		-t[tttt]	change timestamp view	

constructing bpf filters (use with -F or as a string at end of tcpdump command):

ip address	protocol	ports
host A.B.C.D [**src**|**dst**] A.B.C.D [**src**|**dst**] **net** A.B.C.D/n	**proto** p defined: **ip**, **tcp**, **udp**, **icmp**, **arp**	[**src**|**dst**] **port** p
indexing	**bit operations & comparison**	**combining**
ip[index**:**length**]** ~ other protocols work too ~ length is 1,2, or 4	**&**, **|**, **>>**, **<<** **<**, **>**, **!=**, **=**	**not**, **or**, **and**

references
protocol specifications: http://www.networksorcery.com/enp
libpcap (C): http://sourceforge.net/projects/libpcap/
libtrace (C): http://research.wand.net.nz/software/libtrace.php
dpkt (python): http://code.google.com/p/dpkt/
sample pcap: http://wiki.wireshark.org/SampleCaptures