TCPDump Cheat Sheet

Basic Syntax:
  tcpdump [options] [expression]

Common Options:
  -i eth0   Capture on interface eth0
  -n   Don’t resolve hostnames (show raw IPs)
  -c 10   Capture only 10 packets
  -r file.pcap   Read packets from saved capture file

Protocol Filters:
  tcpdump tcp   Show only TCP traffic
  tcpdump udp   Show only UDP traffic
  tcpdump arp   Show ARP traffic
  tcpdump icmp   Show ICMP (ping) traffic
  tcpdump port 80   Show traffic on port 80 (HTTP)
  tcpdump portrange 20-25 Show traffic on ports 20-25

Size Filters:
  tcpdump greater 1500   Packets larger than 1500 bytes
  tcpdump less 64   Packets smaller than 64 bytes

IP Filters:
  tcpdump host 192.168.1.10   Packets to/from specific host
  tcpdump src host 192.168.1.10   Packets with given source IP
  tcpdump dst host 192.168.1.10   Packets with given destination IP

Flag Filters:
  tcpdump 'tcp[tcpflags] & tcp-rst != 0'
    Show packets with TCP RST flag set
  tcpdump 'tcp[tcpflags] & tcp-syn != 0'
    Show packets with TCP SYN flag set

Combining Filters:
  tcpdump tcp and port 443
    Show only TCP packets on port 443
  tcpdump src host 10.10.10.5 and dst port 22
    Show packets from 10.10.10.5 going to SSH (port 22)

Tips:
- Always use -n to avoid slow lookups.
- Use filters to reduce noise and focus on what matters.
- Redirect output to a file if you need to parse with tools like awk or grep.