TCP and UDP - Command Cheat Sheet

Wireshark

Filter out a specific port:

- `not tcp.port == 3389`

tcpdump

Command Options:

Flag	Description
-nn	No hostname or port resolution
-r	"Read" in a PCAP

Syntax:

- `tcpdump [OPTIONS] [BPF Filter]`

Filter for packets with SYN and ACK flags set:

- `tcpdump -nn -r simple-https.pcap 'tcp[tcpflags] == (tcp-syn|tcp-ack)'`

Filter and extracting multiple fields example:

- `tcpdump -nn -r simple-https.pcap 'tcp[tcpflags] == (tcp-syn|tcp-ack)' | cut -f 3,7 -d " "`

Combined list of destination ports with a count:

- `tcpdump -nn -r normal-web-traffic.pcap 'src host 192.168.218.131' | cut -f 5 -d " " | cut -f 5 -d "." | sort | uniq -c | sort -n`

Additional BPF Filter examples:

- `src host 192.168.218.131`

- `host 192.168.218.131 and port 123`

Linux Reference

`cut` command options:

Flag	Description
-f	Specifies the field (column)
-d	Specifies the delimiter

"Sort Sandwich":

- `sort | uniq -c | sort -n`