

# Linux

## Live System

*Some of it also work on disk images*

## Process Information

```
/proc/{pid}/          #process
/proc/{pid}/exe       #executable, (also for stopped processes)

/proc/{pid}/cmdline
/proc/{pid}/environ
/proc/{pid}/fd
/proc/{pid}/cwd       # working directory
/proc/{pid}/net
/proc/{pid}/status

# open ports, assume folder /proc/{pid}/
cat ./net/tcp | awk 'NR>1 {split($2, a, ":"); printf "%d\n", "0x" a[2]}'

# local ip's and ports
awk 'NR>1 {
  split($2, a, ":")
  hex = a[1]
  # Extract bytes (IP is little-endian in the file)
  b1 = substr(hex,7,2); b2 = substr(hex,5,2)
  b3 = substr(hex,3,2); b4 = substr(hex,1,2)
  printf "%d.%d.%d.%d:%d\n",
    "0x"b1, "0x"b2, "0x"b3, "0x"b4,
    "0x"a[2]
}' ./net/tcp

# connected local ip's
cat /net/arp
cat /net/route
```

## Basic System Info

```
timedatectl status
lsmod
iptables-save
```

## mount