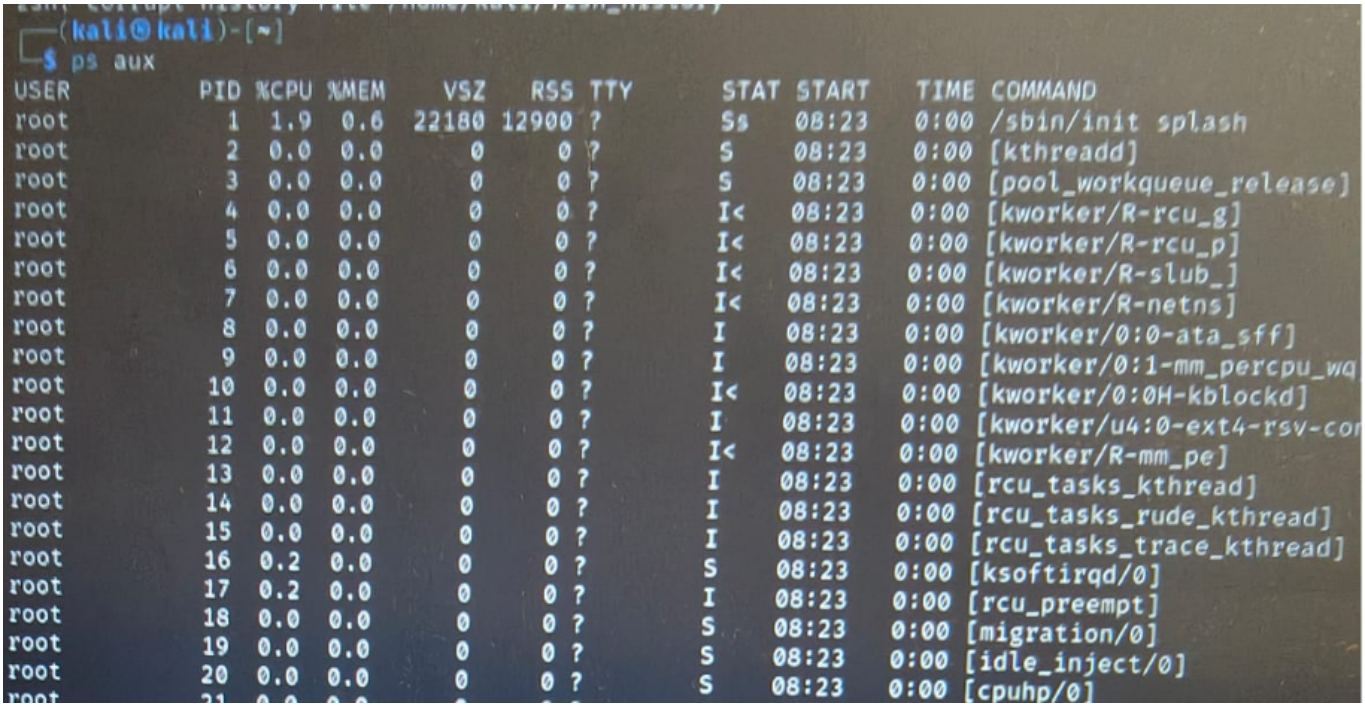
◇ 1. Viewing All Processes

Command: `ps aux` 🖭

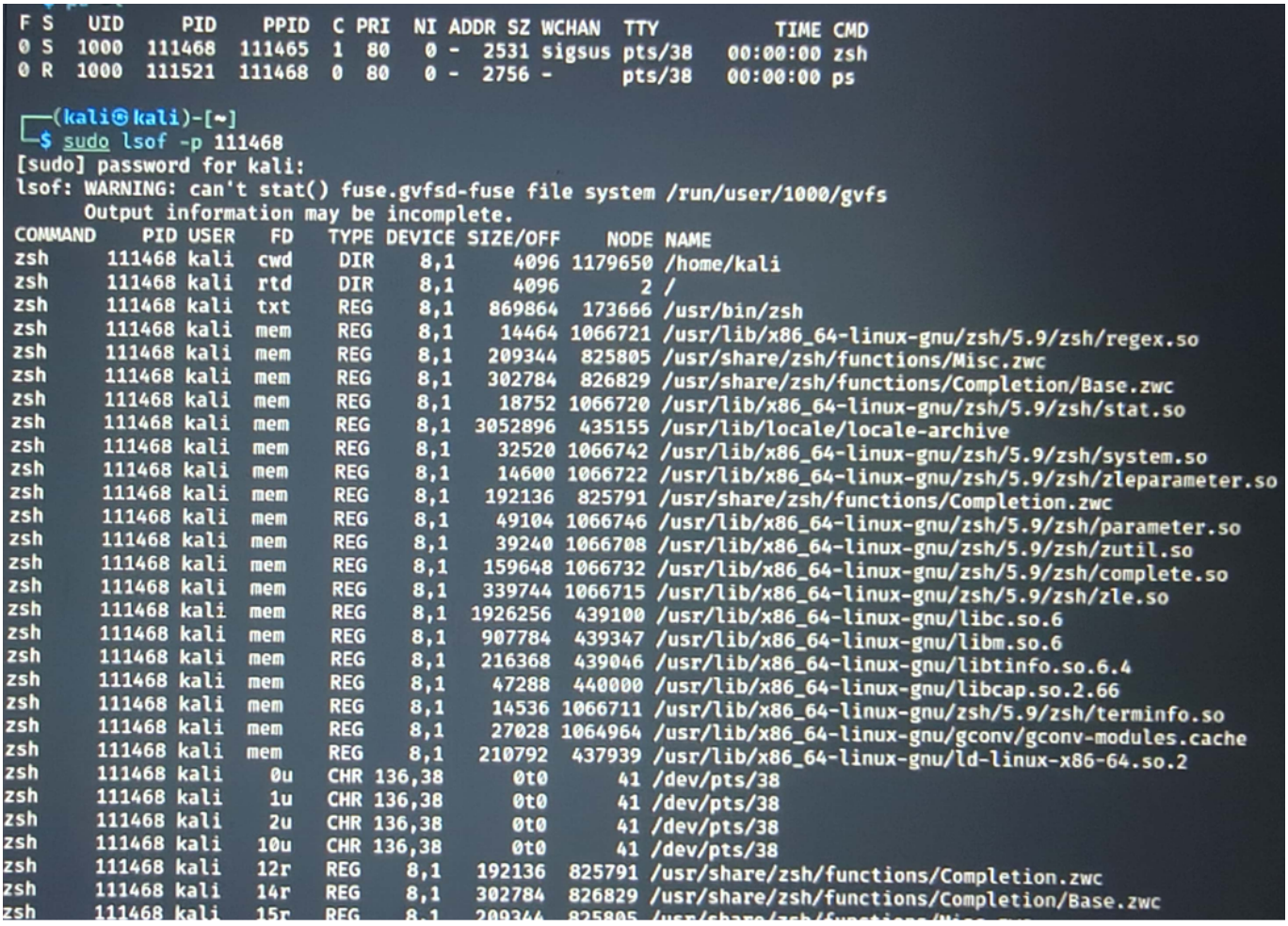


```
┌──(kali㉿kali)-[~]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  1.9  0.6  22180 12900 ?        Ss   08:23   0:00 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    08:23   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    08:23   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   08:23   0:00 [kworker/R-rcu_g]
root           5  0.0  0.0      0     0 ?        I<   08:23   0:00 [kworker/R-rcu_p]
root           6  0.0  0.0      0     0 ?        I<   08:23   0:00 [kworker/R-slub_]
root           7  0.0  0.0      0     0 ?        I<   08:23   0:00 [kworker/R-netns]
root           8  0.0  0.0      0     0 ?        I    08:23   0:00 [kworker/0:0-ata_sff]
root           9  0.0  0.0      0     0 ?        I    08:23   0:00 [kworker/0:1-mm_percpu_wq
root          10  0.0  0.0      0     0 ?        I<   08:23   0:00 [kworker/0:0H-kblockd]
root          11  0.0  0.0      0     0 ?        I    08:23   0:00 [kworker/u4:0-ext4-rsv-co
root          12  0.0  0.0      0     0 ?        I<   08:23   0:00 [kworker/R-mm_pe]
root          13  0.0  0.0      0     0 ?        I    08:23   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    08:23   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    08:23   0:00 [rcu_tasks_trace_kthread]
root          16  0.2  0.0      0     0 ?        S    08:23   0:00 [ksoftirqd/0]
root          17  0.2  0.0      0     0 ?        I    08:23   0:00 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    08:23   0:00 [migration/0]
root          19  0.0  0.0      0     0 ?        S    08:23   0:00 [idle_inject/0]
root          20  0.0  0.0      0     0 ?        S    08:23   0:00 [cpuhp/0]
```

:

♙ 2. Process Tree

Command: `pstree -p` 🖭



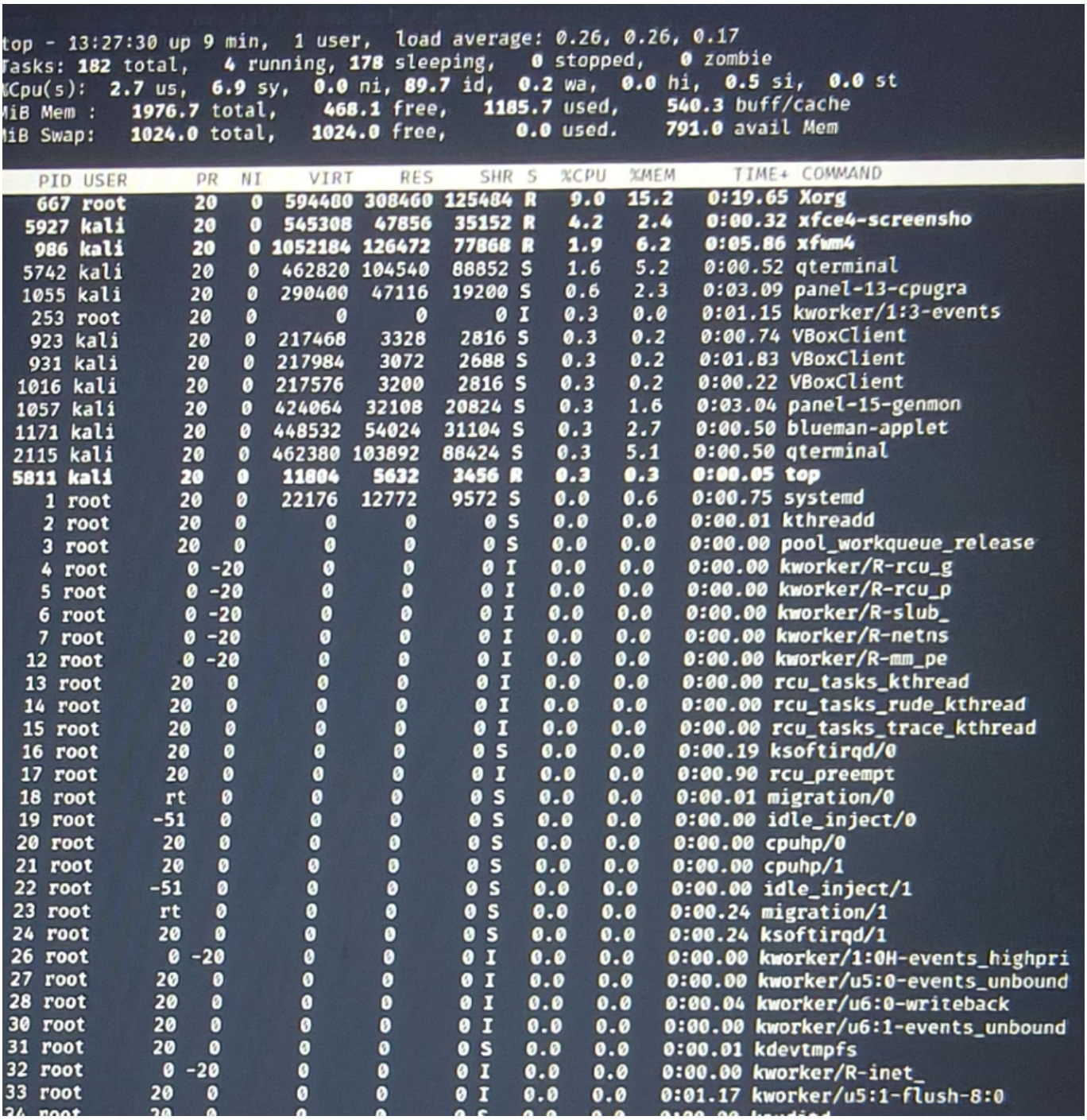
```
F S   UID     PID    PPID  C PRI  NI ADDR SZ WCHAN  TTY          TIME CMD
0 S  1000  111468  111465  1  80   0 -  2531 sigsus pts/38   00:00:00 zsh
0 R  1000  111521  111468  0  80   0 -  2756 -      pts/38   00:00:00 ps

┌──(kali㉿kali)-[~]
└─$ sudo lsof -p 111468
[sudo] password for kali:
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
COMMAND    PID USER   FD   TYPE DEVICE SIZE/OFF    NODE NAME
zsh     111468 kali  cwd    DIR    8,1     4096 1179650 /home/kali
zsh     111468 kali  rtd    DIR    8,1     4096       2 /
zsh     111468 kali  txt    REG    8,1   869864  173666 /usr/bin/zsh
zsh     111468 kali  mem    REG    8,1    14464 1066721 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/regex.so
zsh     111468 kali  mem    REG    8,1   209344  825805 /usr/share/zsh/functions/Misc.zwc
zsh     111468 kali  mem    REG    8,1   302784  826829 /usr/share/zsh/functions/Completion/Base.zwc
zsh     111468 kali  mem    REG    8,1    18752 1066720 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/stat.so
zsh     111468 kali  mem    REG    8,1  3052896  435155 /usr/lib/locale/locale-archive
zsh     111468 kali  mem    REG    8,1    32520 1066742 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/system.so
zsh     111468 kali  mem    REG    8,1    14600 1066722 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/zleparameter.so
zsh     111468 kali  mem    REG    8,1   192136  825791 /usr/share/zsh/functions/Completion.zwc
zsh     111468 kali  mem    REG    8,1    49104 1066746 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/parameter.so
zsh     111468 kali  mem    REG    8,1    39240 1066708 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/zutil.so
zsh     111468 kali  mem    REG    8,1   159648 1066732 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/complete.so
zsh     111468 kali  mem    REG    8,1   339744 1066715 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/zle.so
zsh     111468 kali  mem    REG    8,1  1926256  439100 /usr/lib/x86_64-linux-gnu/libc.so.6
zsh     111468 kali  mem    REG    8,1   907784  439347 /usr/lib/x86_64-linux-gnu/libm.so.6
zsh     111468 kali  mem    REG    8,1   216368  439046 /usr/lib/x86_64-linux-gnu/libtinfo.so.6.4
zsh     111468 kali  mem    REG    8,1    47288  440000 /usr/lib/x86_64-linux-gnu/libcap.so.2.66
zsh     111468 kali  mem    REG    8,1    14536 1066711 /usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/terminfo.so
zsh     111468 kali  mem    REG    8,1    27028 1064964 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
zsh     111468 kali  mem    REG    8,1   210792  437939 /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
zsh     111468 kali    0u   CHR 136,38      0t0      41 /dev/pts/38
zsh     111468 kali    1u   CHR 136,38      0t0      41 /dev/pts/38
zsh     111468 kali    2u   CHR 136,38      0t0      41 /dev/pts/38
zsh     111468 kali   10u   CHR 136,38      0t0      41 /dev/pts/38
zsh     111468 kali   12r   REG    8,1   192136  825791 /usr/share/zsh/functions/Completion.zwc
zsh     111468 kali   14r   REG    8,1   302784  826829 /usr/share/zsh/functions/Completion/Base.zwc
```

:

3. Real-Time Process Monitoring

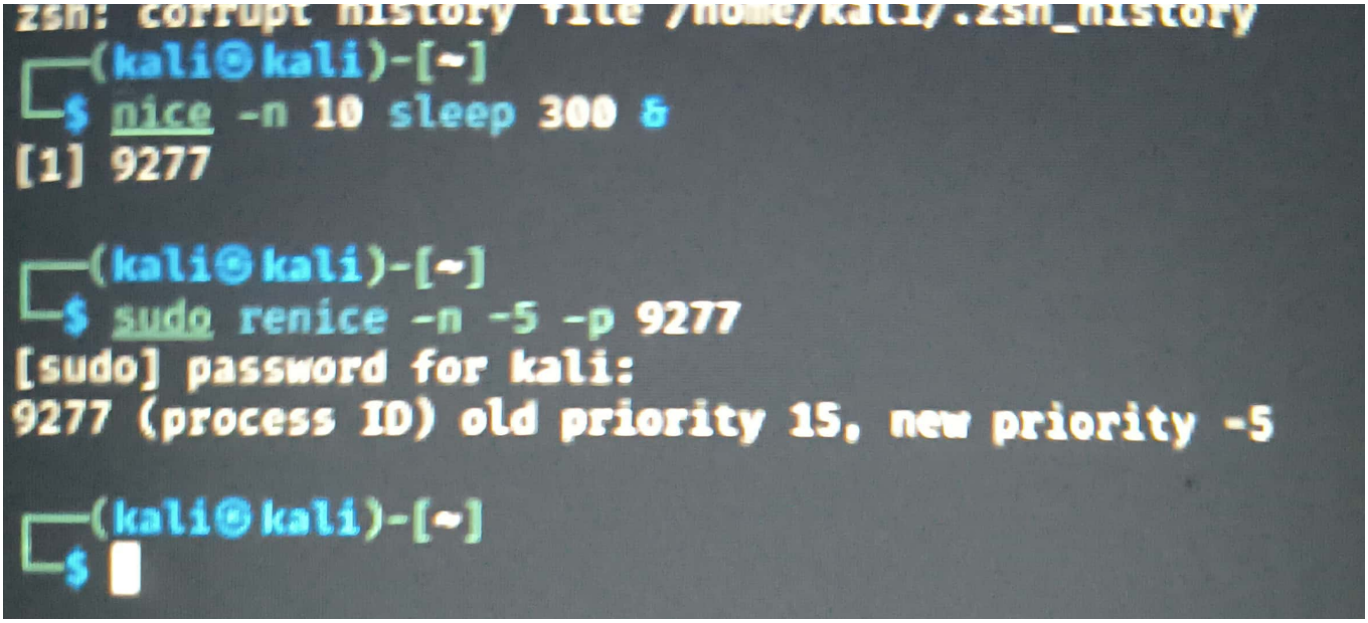
Command: `top`



: *

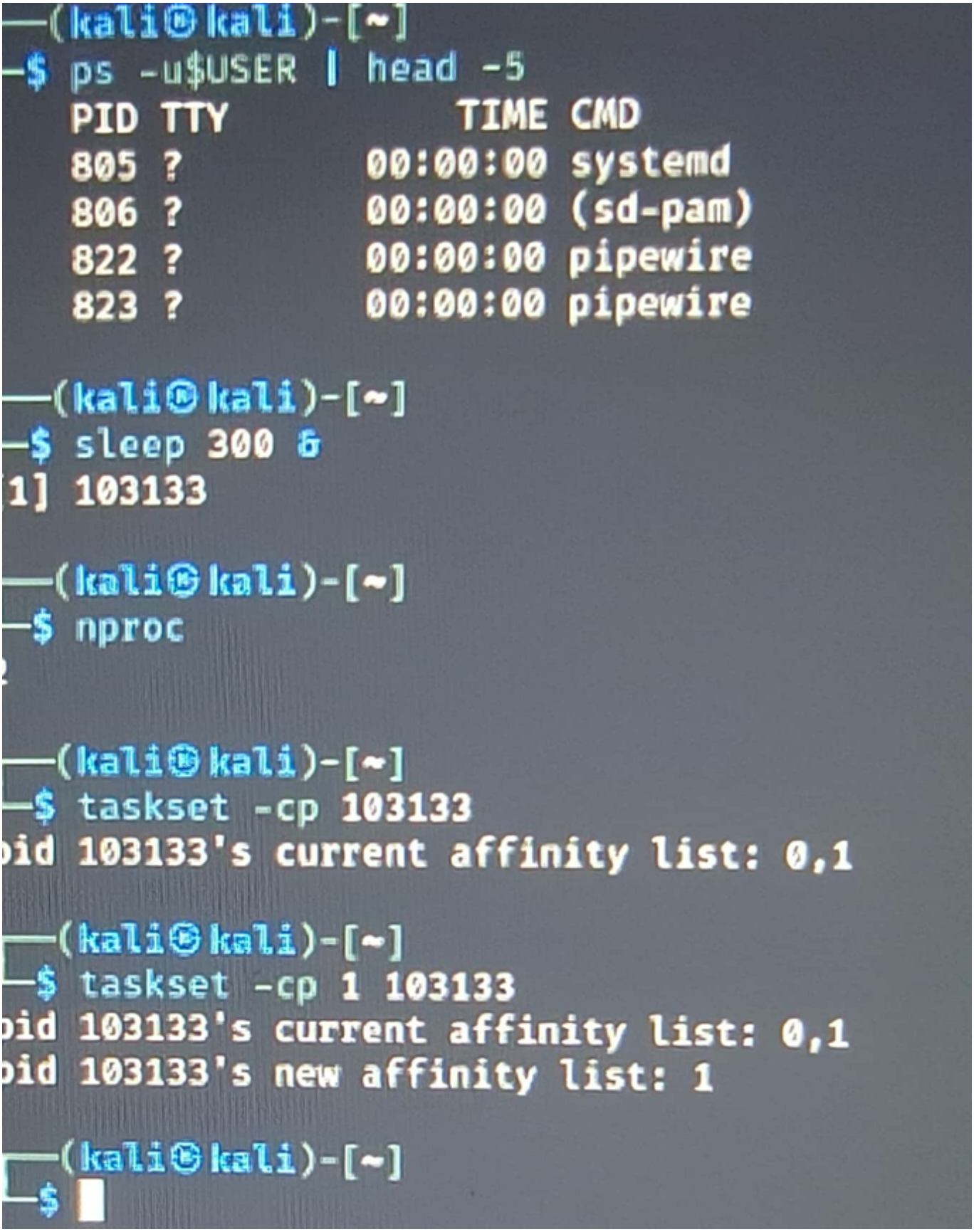
4. Adjusting Process Priority

Command 1: `nice -n 10 sleep 300 &` **Command 2:** `renice -n -5 -p 3050` 📸



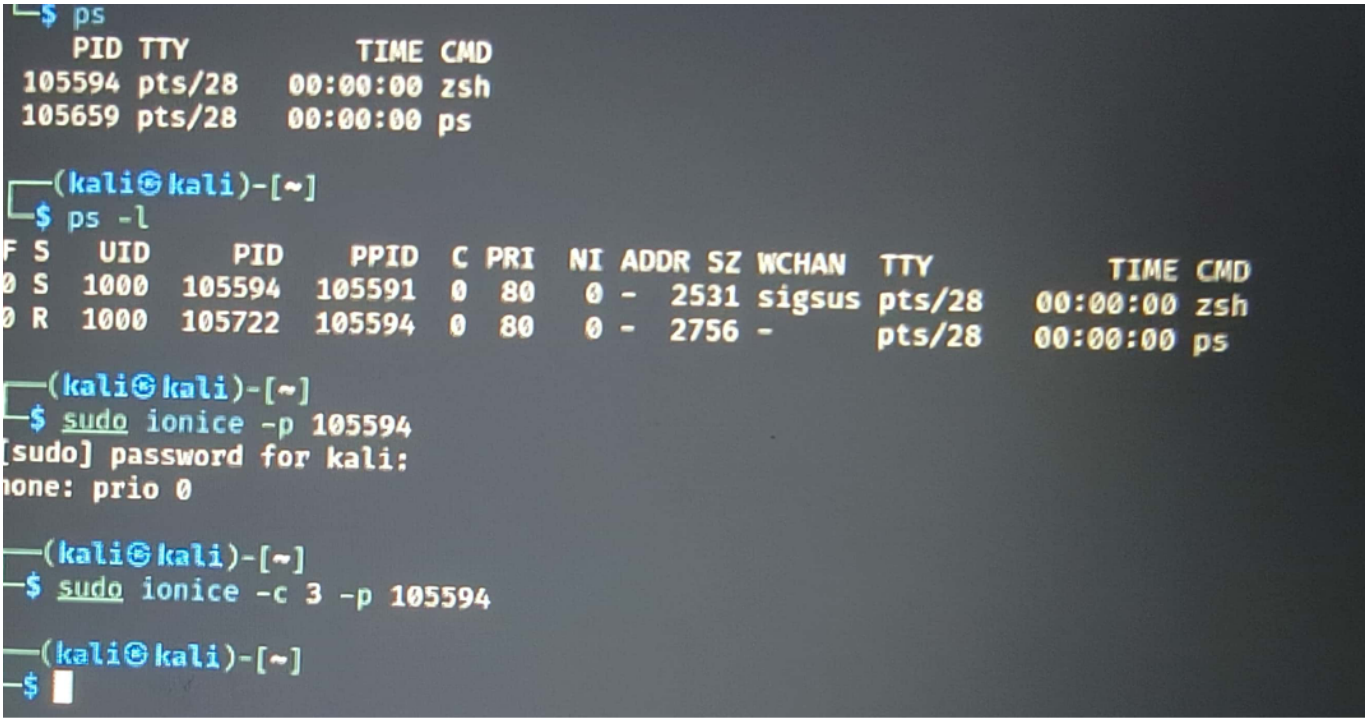
🔧 5. CPU Affinity

Command 1: `taskset -cp 3050` **Command 2:** `taskset -cp 1 3050` 🖻



🗁 6. I/O Scheduling Priority

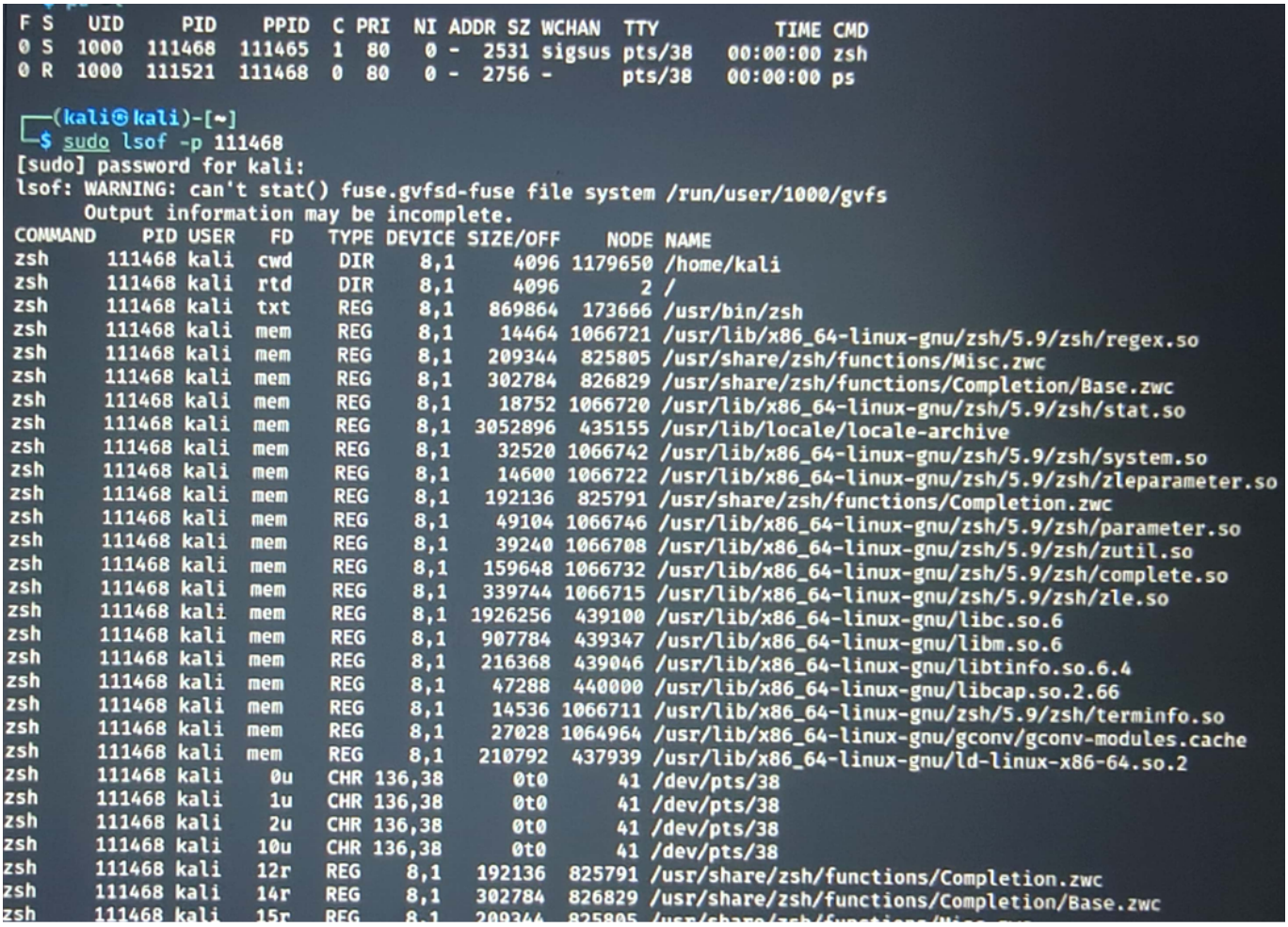
Command: `ionice -c 3 -p 3050` 📸



---

7. File Descriptors Used by a Process

Command: `lsof -p 3050 | head -5` 📸



---

8. Trace System Calls of a Process

Command: `strace -p 3050`

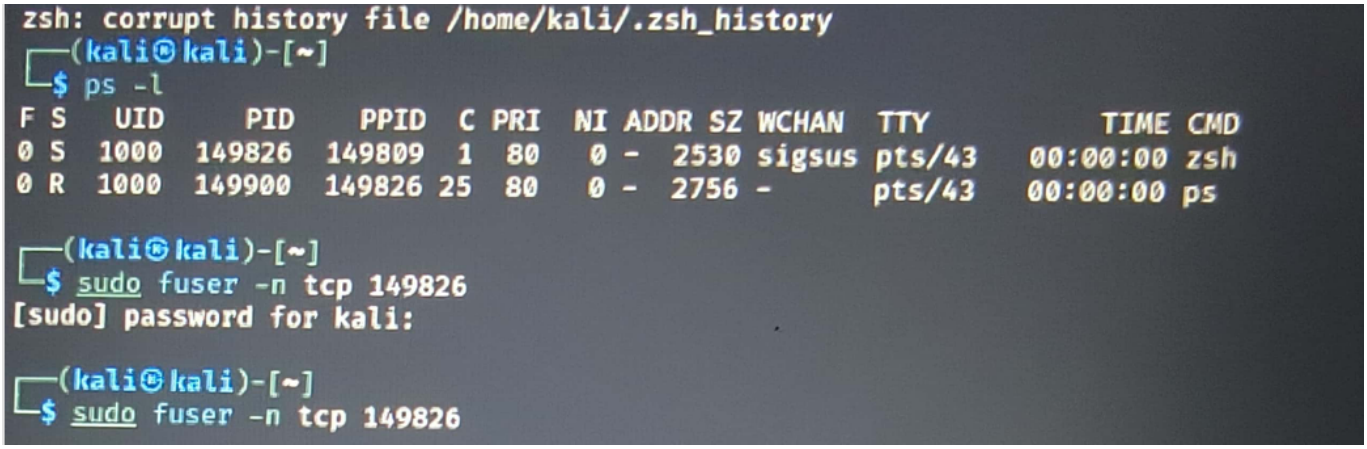
```
kali@kali:~$ strace -p 3050
strace: Process 3050 attached
restart_syscall(<... resuming interrupted nanosleep
...>) = 0
nanosleep({tv_sec=300, tv_nsec=0}, 0x7ffd4a60d8b0)
= ? ERESTART_RESTARTBLOCK (Interrupted by signal)
kali@kali:~$
```

:

---

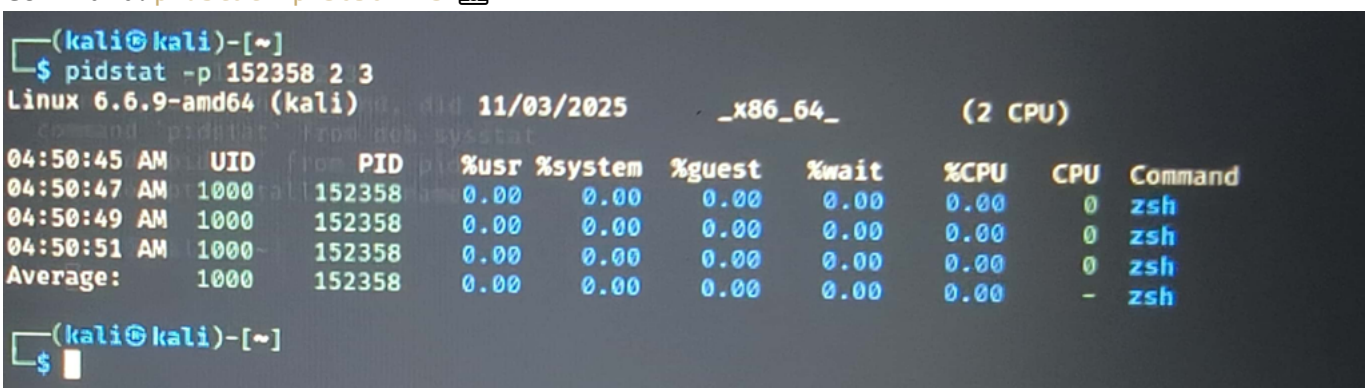
9. Find Process Using a Port

Command: `sudo fuser -n tcp 8080`



10. Per-Process Statistics

Command: `pidstat -p 3050 2 3`



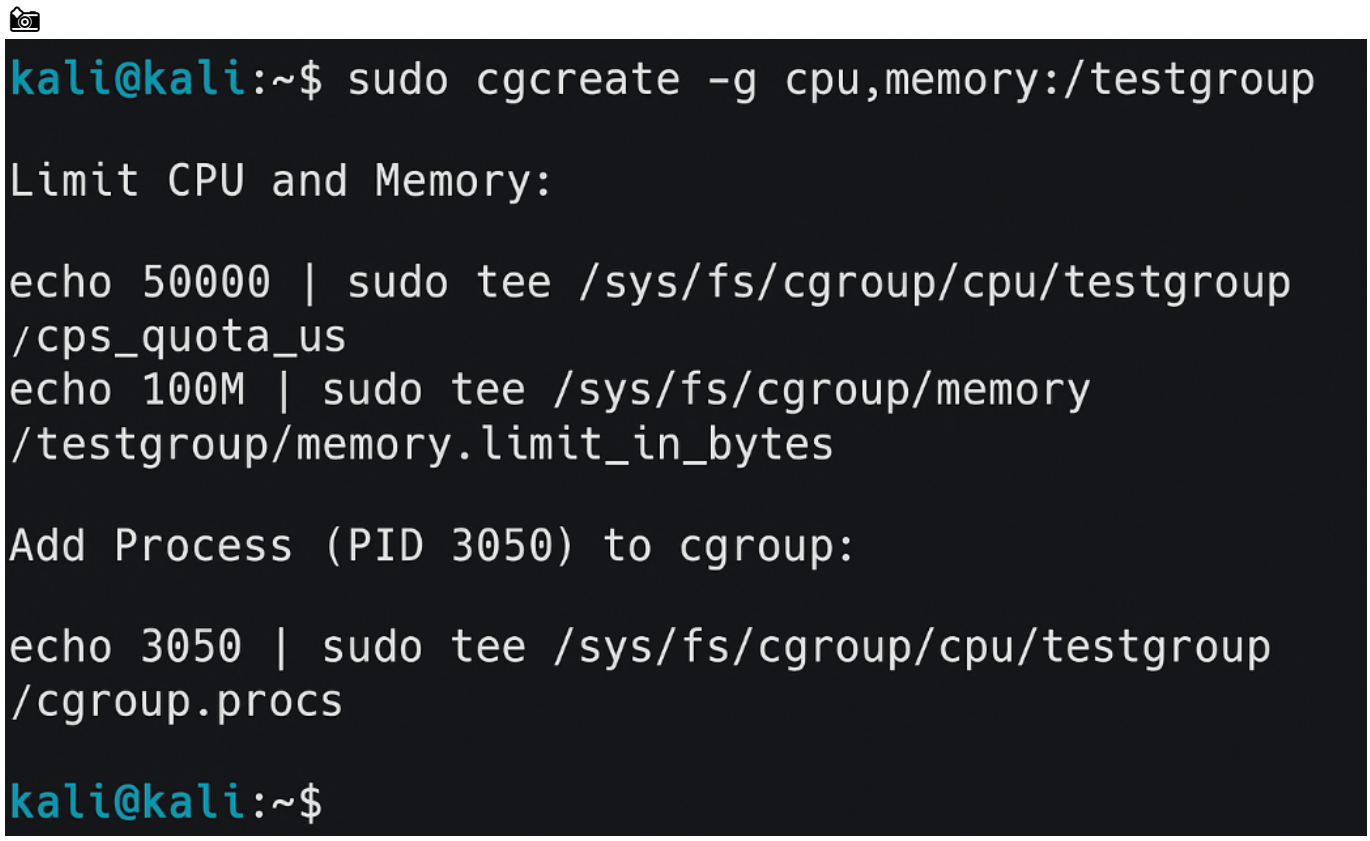
---

11. Control Groups (cgroups)

Command Sequence:

```
sudo cgcreate -g cpu,memory:/testgroup
echo 50000 | sudo tee /sys/fs/cgroup/cpu/testgroup/cpu.cfs_quota_us
```

```
echo 100M | sudo tee /sys/fs/cgroup/memory/testgroup/memory.limit_in_bytes
echo 3050 | sudo tee /sys/fs/cgroup/cpu/testgroup/cgroup.procs
```



---

12. Alternatives to nice / renice

You can show **one example** among these for demonstration, like: `sudo chrt -f 50 sleep 1000`