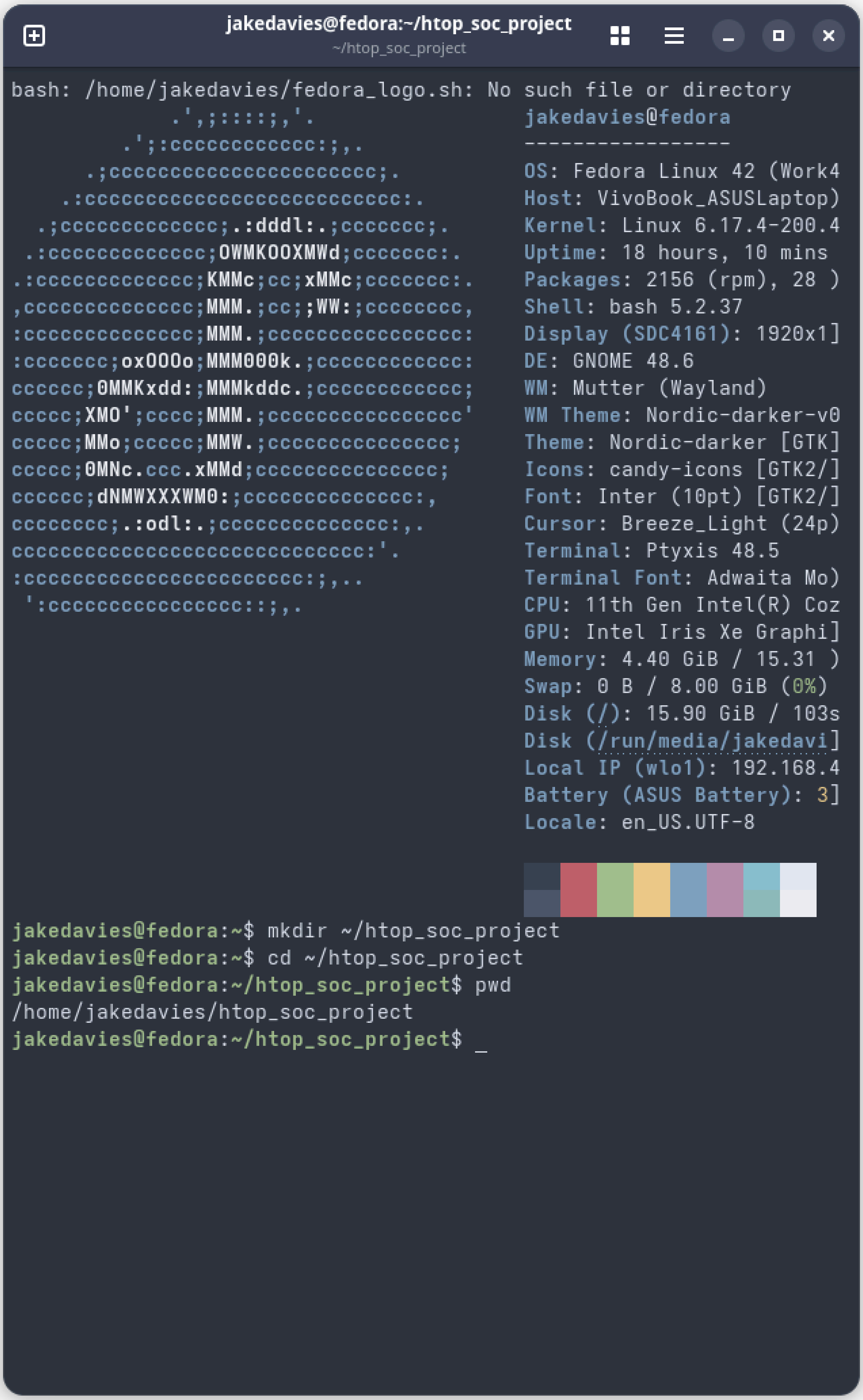
Monitor System Processes with htop to Simulate SOC Triage

Step 1 - Setup:

Firstly i created a new directory with the mkdir command and then changed into the new directory with cd ~/ [directory name]

After i used pwd to confirm where i am.

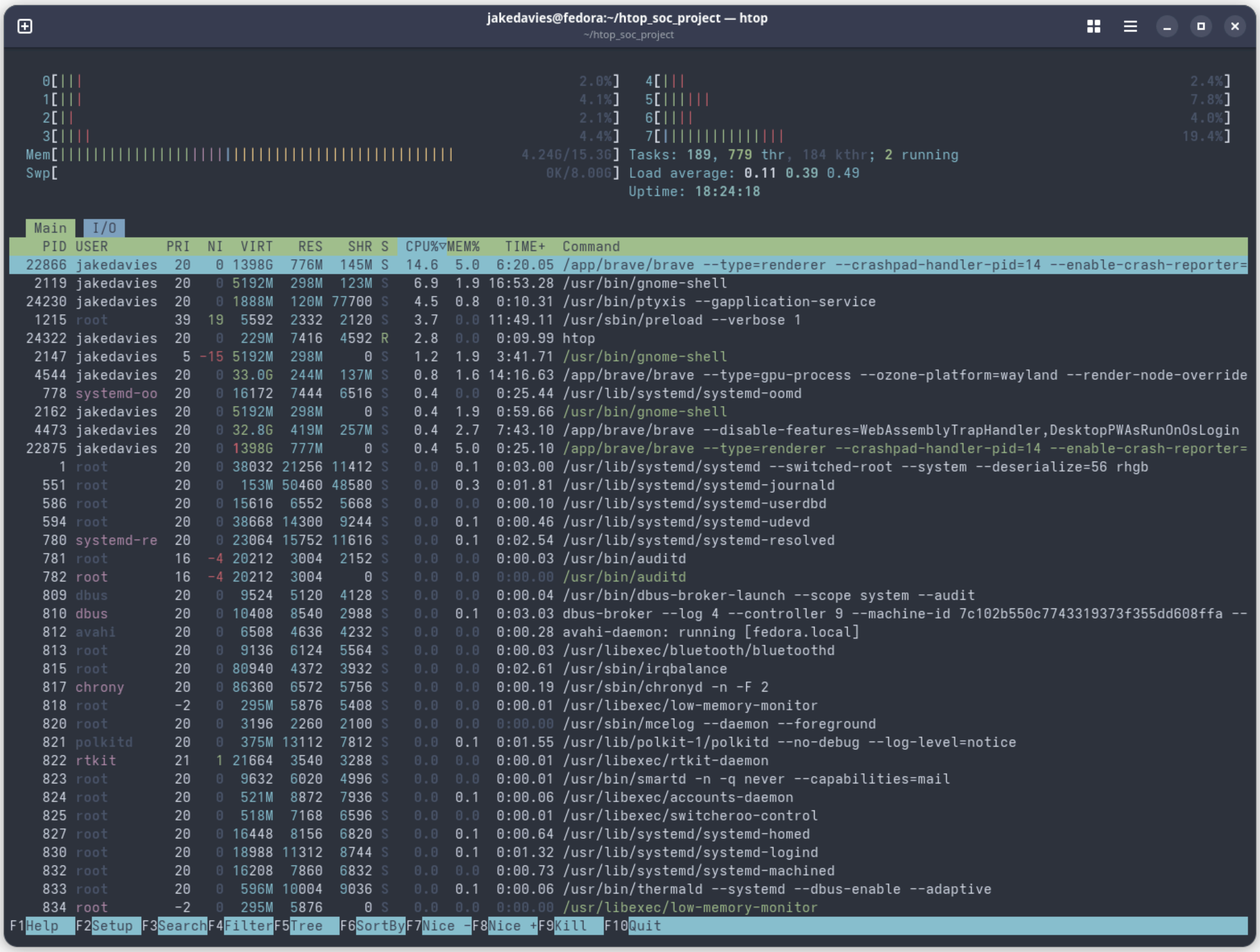


```
bash: /home/jakedavies/fedora_logo.sh: No such file or directory
             .',;::::;,'.                 jakedavies@fedora
         .';:cccccccccccc:;,.             -----------------
      .;cccccccccccccccccccccc;.          OS: Fedora Linux 42 (Work4
    .:cccccccccccccccccccccccccc:.        Host: VivoBook_ASUSLaptop)
  .;ccccccccccccc;.:dddl:.;ccccccc;.      Kernel: Linux 6.17.4-200.4
 .:ccccccccccccc;OWMKOOXMWd;ccccccc:.     Uptime: 18 hours, 10 mins
.:ccccccccccccc;KMMc;cc;xMMc;ccccccc:.    Packages: 2156 (rpm), 28 )
,cccccccccccccc;MMM.;cc;;WW:;cccccccc,    Shell: bash 5.2.37
:cccccccccccccc;MMM.;cccccccccccccccc:    Display (SDC4161): 1920x1]
:ccccccc;oxOOOo;MMM000k.;cccccccccccc:    DE: GNOME 48.6
cccccc;0MMKxdd:;MMMkddc.;cccccccccccc;    WM: Mutter (Wayland)
ccccc;XMO';cccc;MMM.;cccccccccccccccc'    WM Theme: Nordic-darker-v0
ccccc;MMo;ccccc;MMW.;ccccccccccccccc;     Theme: Nordic-darker [GTK]
ccccc;0MNc.ccc.xMMd;ccccccccccccccc;      Icons: candy-icons [GTK2/]
cccccc;dNMWXXXWM0:;cccccccccccccc:,       Font: Inter (10pt) [GTK2/]
cccccccc;.:odl:.;cccccccccccccc:,.        Cursor: Breeze_Light (24p)
ccccccccccccccccccccccccccccccc:'.        Terminal: Ptyxis 48.5
:ccccccccccccccccccccccc:;,..             Terminal Font: Adwaita Mo)
 ':cccccccccccccccc::;,.                  CPU: 11th Gen Intel(R) Coz
                                          GPU: Intel Iris Xe Graphi]
                                          Memory: 4.40 GiB / 15.31 )
                                          Swap: 0 B / 8.00 GiB (0%)
                                          Disk (/): 15.90 GiB / 103s
                                          Disk (/run/media/jakedavi]
                                          Local IP (wlo1): 192.168.4
                                          Battery (ASUS Battery): 3]
                                          Locale: en_US.UTF-8



jakedavies@fedora:~$ mkdir ~/htop_soc_project
jakedavies@fedora:~$ cd ~/htop_soc_project
jakedavies@fedora:~/htop_soc_project$ pwd
/home/jakedavies/htop_soc_project
jakedavies@fedora:~/htop_soc_project$ _
```

Step 2 - Open Htop

On the terminal i type htop to open the program.

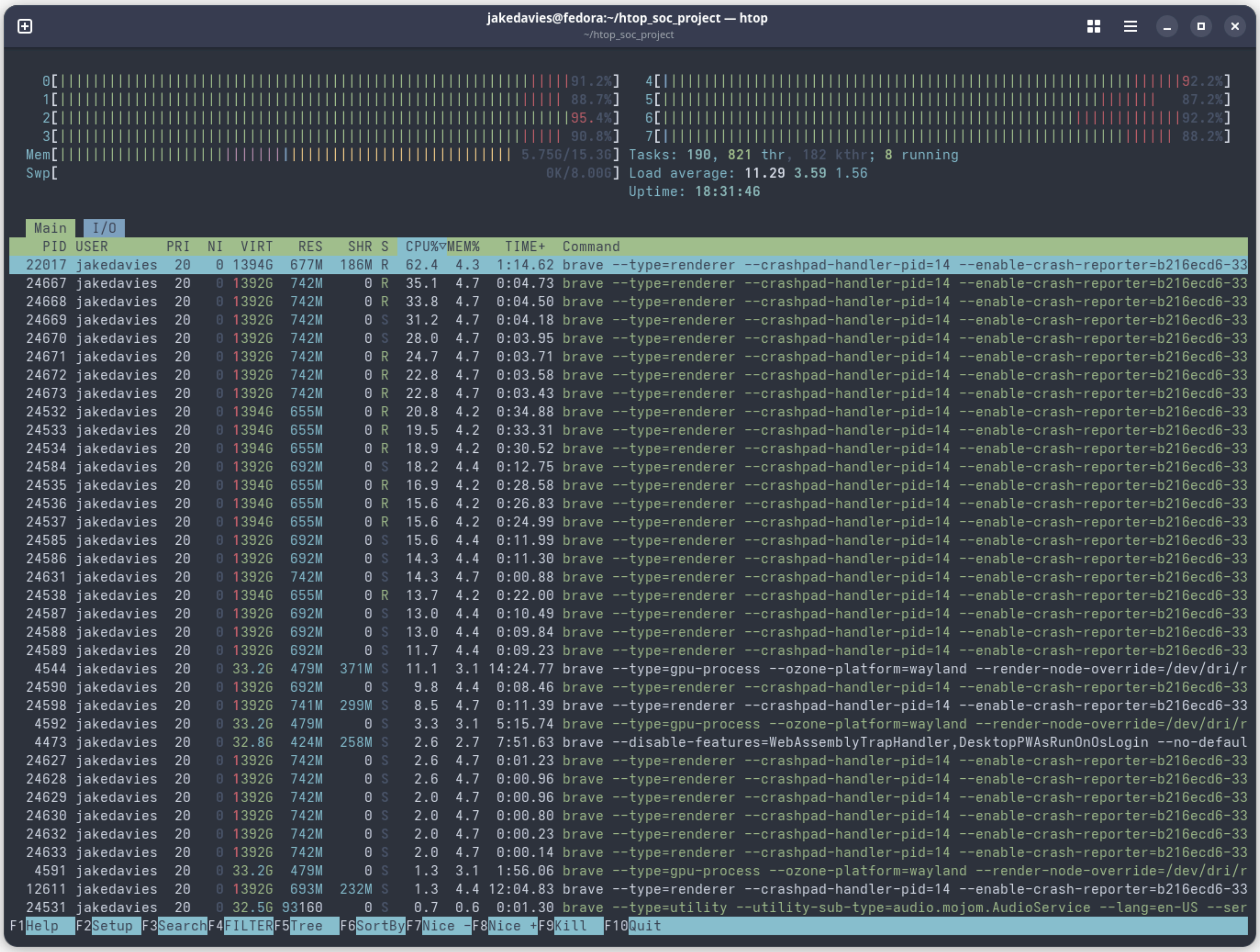
Once on i filter the process using F6 and selecting CPU. This then shows higher usage process jumping to the top making it easier to discover.



jakedavies@fedora:~/htop_soc_project — htop
~/htop_soc_project

```
    0[|||                                                          2.0%]   4[|||                                              2.4%]
    1[|||                                                          4.1%]   5[||||||                                           7.8%]
    2[||                                                           2.1%]   6[||||                                             4.0%]
    3[||||                                                         4.4%]   7[||||||||||||||                                  19.4%]
  Mem[||||||||||||||||||||||||||||||||||||||||||||||||    4.24G/15.3G] Tasks: 189, 779 thr, 184 kthr; 2 running
  Swp[                                                         0K/8.00G] Load average: 0.11 0.39 0.49
                                                                         Uptime: 18:24:18

  Main   I/O
    PID USER       PRI  NI  VIRT   RES   SHR S  CPU%▽MEM%   TIME+  Command
  22866 jakedavies  20   0 1398G  776M  145M S  14.6  5.0  6:20.05 /app/brave/brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=
   2119 jakedavies  20   0 5192M  298M  123M S   6.9  1.9 16:53.28 /usr/bin/gnome-shell
  24230 jakedavies  20   0 1888M  120M 77700 S   4.5  0.8  0:10.31 /usr/bin/ptyxis --gapplication-service
   1215 root        39  19  5592  2332  2120 S   3.7  0.0 11:49.11 /usr/sbin/preload --verbose 1
  24322 jakedavies  20   0  229M  7416  4592 R   2.8  0.0  0:09.99 htop
   2147 jakedavies   5 -15 5192M  298M     0 S   1.2  1.9  3:41.71 /usr/bin/gnome-shell
   4544 jakedavies  20   0 33.0G  244M  137M S   0.8  1.6 14:16.63 /app/brave/brave --type=gpu-process --ozone-platform=wayland --render-node-override
    778 systemd-oo  20   0 16172  7444  6516 S   0.4  0.0  0:25.44 /usr/lib/systemd/systemd-oomd
   2162 jakedavies  20   0 5192M  298M     0 S   0.4  1.9  0:59.66 /usr/bin/gnome-shell
   4473 jakedavies  20   0 32.8G  419M  257M S   0.4  2.7  7:43.10 /app/brave/brave --disable-features=WebAssemblyTrapHandler,DesktopPWAsRunOnOsLogin
  22875 jakedavies  20   0 1398G  777M     0 S   0.4  5.0  0:25.10 /app/brave/brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=
      1 root        20   0 38032 21256 11412 S   0.0  0.1  0:03.00 /usr/lib/systemd/systemd --switched-root --system --deserialize=56 rhgb
    551 root        20   0  153M 50460 48580 S   0.0  0.3  0:01.81 /usr/lib/systemd/systemd-journald
    586 root        20   0 15616  6552  5668 S   0.0  0.0  0:00.10 /usr/lib/systemd/systemd-userdbd
    594 root        20   0 38668 14300  9244 S   0.0  0.1  0:00.46 /usr/lib/systemd/systemd-udevd
    780 systemd-re  20   0 23064 15752 11616 S   0.0  0.1  0:02.54 /usr/lib/systemd/systemd-resolved
    781 root        16  -4 20212  3004  2152 S   0.0  0.0  0:00.03 /usr/bin/auditd
    782 root        16  -4 20212  3004     0 S   0.0  0.0  0:00.00 /usr/bin/auditd
    809 dbus        20   0  9524  5120  4128 S   0.0  0.0  0:00.04 /usr/bin/dbus-broker-launch --scope system --audit
    810 dbus        20   0 10408  8540  2988 S   0.0  0.1  0:03.03 dbus-broker --log 4 --controller 9 --machine-id 7c102b550c7743319373f355dd608ffa --
    812 avahi       20   0  6508  4636  4232 S   0.0  0.0  0:00.28 avahi-daemon: running [fedora.local]
    813 root        20   0  9136  6124  5564 S   0.0  0.0  0:00.03 /usr/libexec/bluetooth/bluetoothd
    815 root        20   0 80940  4372  3932 S   0.0  0.0  0:02.61 /usr/sbin/irqbalance
    817 chrony      20   0 86360  6572  5756 S   0.0  0.0  0:00.19 /usr/sbin/chronyd -n -F 2
    818 root        -2   0  295M  5876  5408 S   0.0  0.0  0:00.01 /usr/libexec/low-memory-monitor
    820 root        20   0  3196  2260  2100 S   0.0  0.0  0:00.00 /usr/sbin/mcelog --daemon --foreground
    821 polkitd     20   0  375M 13112  7812 S   0.0  0.1  0:01.55 /usr/lib/polkit-1/polkitd --no-debug --log-level=notice
    822 rtkit       21   1 21664  3540  3288 S   0.0  0.0  0:00.01 /usr/libexec/rtkit-daemon
    823 root        20   0  9632  6020  4996 S   0.0  0.0  0:00.01 /usr/bin/smartd -n -q never --capabilities=mail
    824 root        20   0  521M  8872  7936 S   0.0  0.1  0:00.06 /usr/libexec/accounts-daemon
    825 root        20   0  518M  7168  6596 S   0.0  0.0  0:00.01 /usr/libexec/switcheroo-control
    827 root        20   0 16448  8156  6820 S   0.0  0.1  0:00.64 /usr/lib/systemd/systemd-homed
    830 root        20   0 18988 11312  8744 S   0.0  0.1  0:01.32 /usr/lib/systemd/systemd-logind
    832 root        20   0 16208  7860  6832 S   0.0  0.0  0:00.73 /usr/lib/systemd/systemd-machined
    833 root        20   0  596M 10004  9036 S   0.0  0.1  0:00.06 /usr/bin/thermald --systemd --dbus-enable --adaptive
    834 root        -2   0  295M  5876     0 S   0.0  0.0  0:00.00 /usr/libexec/low-memory-monitor
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

After this i then press F4 to type Brave to only show Brave processes. Thus cutting out the noise.



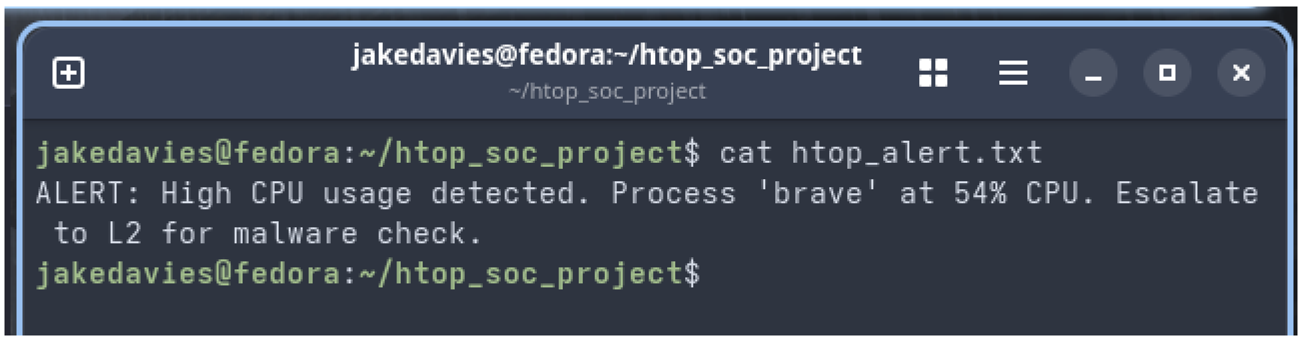
```
    0[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||91.2%]   4[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||92.2%]
    1[|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||| 88.7%]   5[|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||   87.2%]
    2[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||95.4%]   6[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||92.2%]
    3[|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||| 90.8%]   7[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||| 88.2%]
  Mem[||||||||||||||||||||||||||||||||||||||||||||||||||||||| 5.75G/15.3G] Tasks: 190, 821 thr, 182 kthr; 8 running
  Swp[                                                          0K/8.00G] Load average: 11.29 3.59 1.56
                                                                           Uptime: 18:31:46

  Main  I/O
    PID USER       PRI  NI  VIRT   RES   SHR S  CPU%▽MEM%   TIME+  Command
  22017 jakedavies  20   0 1394G  677M  186M R  62.4  4.3  1:14.62 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24667 jakedavies  20   0 1392G  742M     0 R  35.1  4.7  0:04.73 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24668 jakedavies  20   0 1392G  742M     0 R  33.8  4.7  0:04.50 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24669 jakedavies  20   0 1392G  742M     0 S  31.2  4.7  0:04.18 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24670 jakedavies  20   0 1392G  742M     0 S  28.0  4.7  0:03.95 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24671 jakedavies  20   0 1392G  742M     0 R  24.7  4.7  0:03.71 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24672 jakedavies  20   0 1392G  742M     0 R  22.8  4.7  0:03.58 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24673 jakedavies  20   0 1392G  742M     0 R  22.8  4.7  0:03.43 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24532 jakedavies  20   0 1394G  655M     0 R  20.8  4.2  0:34.88 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24533 jakedavies  20   0 1394G  655M     0 R  19.5  4.2  0:33.31 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24534 jakedavies  20   0 1394G  655M     0 R  18.9  4.2  0:30.52 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24584 jakedavies  20   0 1392G  692M     0 S  18.2  4.4  0:12.75 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24535 jakedavies  20   0 1394G  655M     0 R  16.9  4.2  0:28.58 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24536 jakedavies  20   0 1394G  655M     0 R  15.6  4.2  0:26.83 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24537 jakedavies  20   0 1394G  655M     0 R  15.6  4.2  0:24.99 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24585 jakedavies  20   0 1392G  692M     0 S  15.6  4.4  0:11.99 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24586 jakedavies  20   0 1392G  692M     0 S  14.3  4.4  0:11.30 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24631 jakedavies  20   0 1392G  742M     0 S  14.3  4.7  0:00.88 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24538 jakedavies  20   0 1394G  655M     0 R  13.7  4.2  0:22.00 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24587 jakedavies  20   0 1392G  692M     0 S  13.0  4.4  0:10.49 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24588 jakedavies  20   0 1392G  692M     0 S  13.0  4.4  0:09.84 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24589 jakedavies  20   0 1392G  692M     0 S  11.7  4.4  0:09.23 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
   4544 jakedavies  20   0 33.2G  479M  371M S  11.1  3.1 14:24.77 brave --type=gpu-process --ozone-platform=wayland --render-node-override=/dev/dri/r
  24590 jakedavies  20   0 1392G  692M     0 S   9.8  4.4  0:08.46 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24598 jakedavies  20   0 1392G  741M  299M S   8.5  4.7  0:11.39 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
   4592 jakedavies  20   0 33.2G  479M     0 S   3.3  3.1  5:15.74 brave --type=gpu-process --ozone-platform=wayland --render-node-override=/dev/dri/r
   4473 jakedavies  20   0 32.8G  424M  258M S   2.6  2.7  7:51.63 brave --disable-features=WebAssemblyTrapHandler,DesktopPWAsRunOnOsLogin --no-defaul
  24627 jakedavies  20   0 1392G  742M     0 S   2.6  4.7  0:01.23 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24628 jakedavies  20   0 1392G  742M     0 S   2.6  4.7  0:00.96 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24629 jakedavies  20   0 1392G  742M     0 S   2.0  4.7  0:00.96 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24630 jakedavies  20   0 1392G  742M     0 S   2.0  4.7  0:00.80 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24632 jakedavies  20   0 1392G  742M     0 S   2.0  4.7  0:00.23 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24633 jakedavies  20   0 1392G  742M     0 S   2.0  4.7  0:00.14 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
   4591 jakedavies  20   0 33.2G  479M     0 S   1.3  3.1  1:56.06 brave --type=gpu-process --ozone-platform=wayland --render-node-override=/dev/dri/r
  12611 jakedavies  20   0 1392G  693M  232M S   1.3  4.4 12:04.83 brave --type=renderer --crashpad-handler-pid=14 --enable-crash-reporter=b216ecd6-33
  24531 jakedavies  20   0 32.5G 93160     0 S   0.7  0.6  0:01.30 brave --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --ser
F1Help  F2Setup F3SearchF4FILTERF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

As we can see at the top it shows Brave browser with a CPU % of 60+

After i found the high CPU process i then quit htop by pressing q

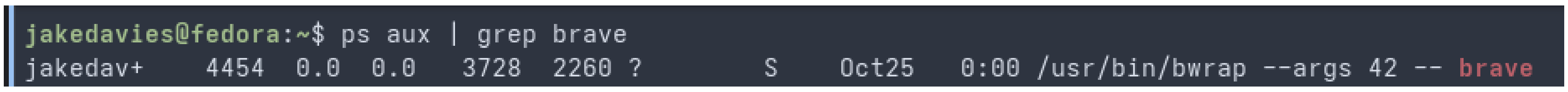
Step 3 - Escalate

Documented the alert using the Echo command tohtop_alert.txt and used cat htop_alert.txt to show it on my terminal.

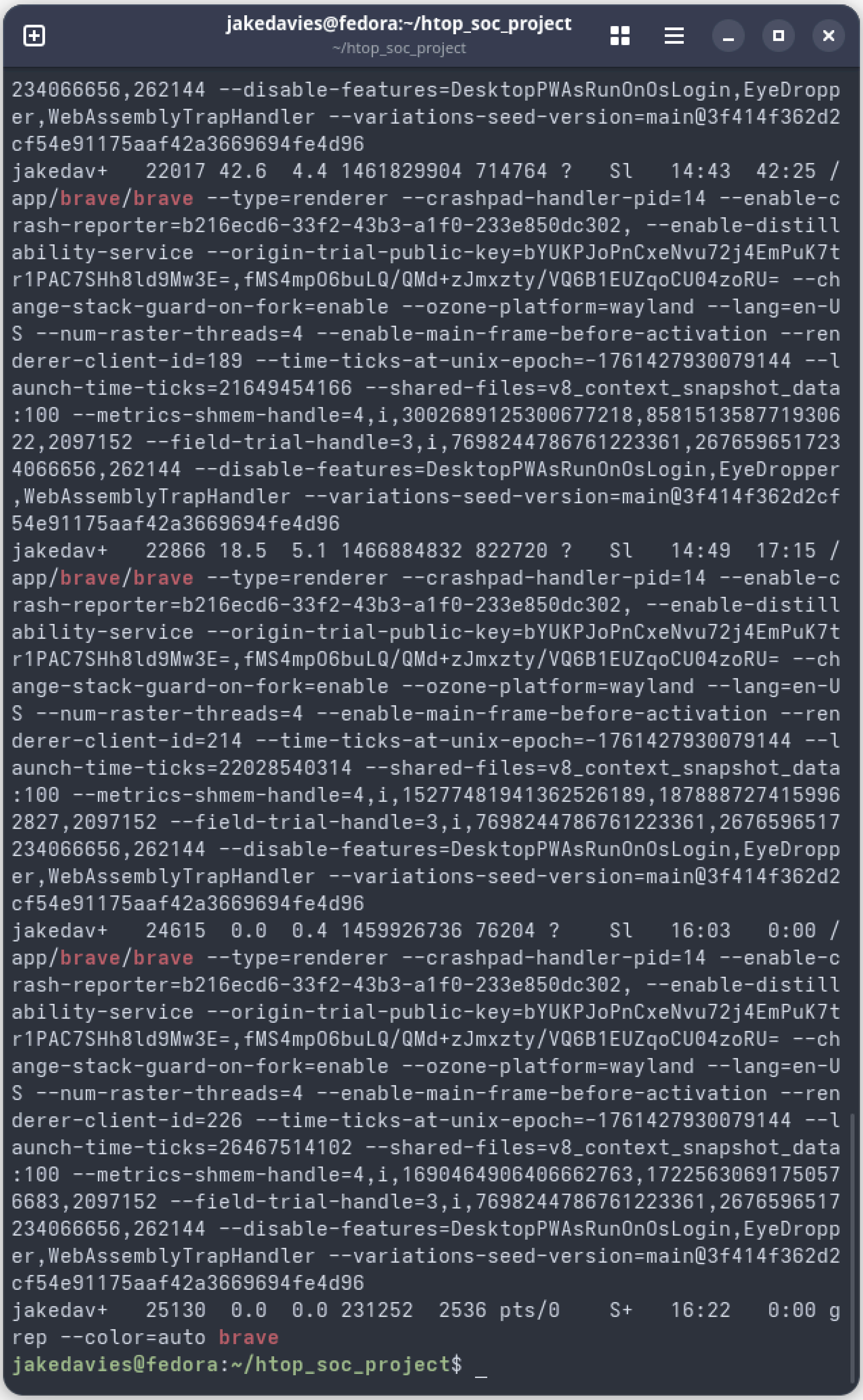


```
jakedavies@fedora:~/htop_soc_project$ cat htop_alert.txt
ALERT: High CPU usage detected. Process 'brave' at 54% CPU. Escalate
 to L2 for malware check.
jakedavies@fedora:~/htop_soc_project$
```

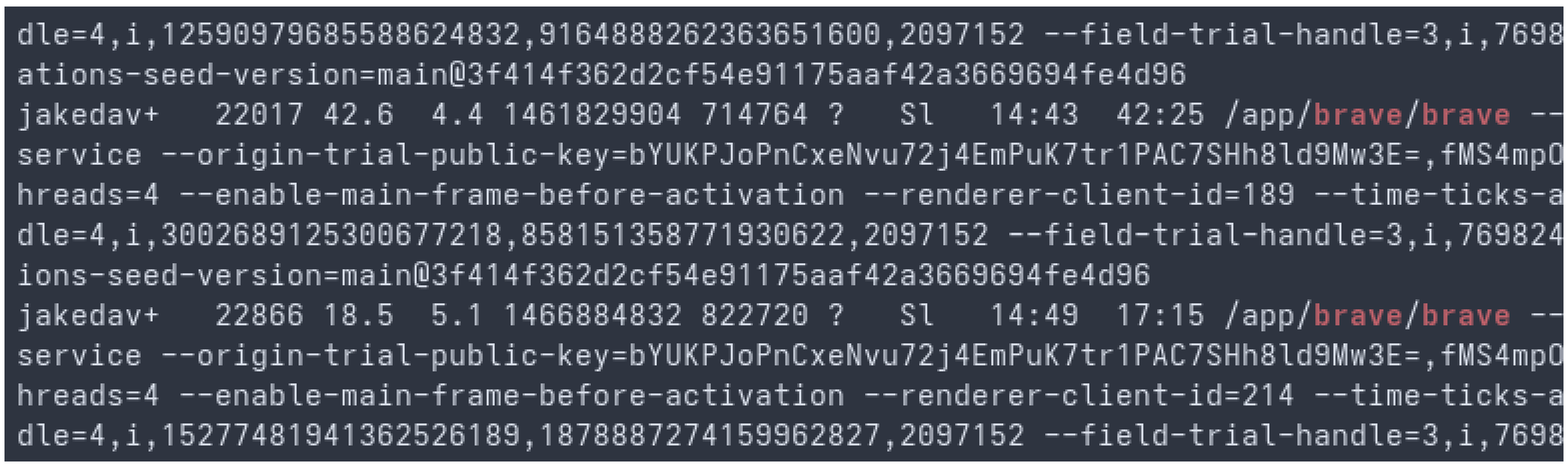
Also i decided to cross check using a new command i learnt which is **ps aux | grep [process name]



```
jakedavies@fedora:~$ ps aux | grep brave
jakedav+     4454  0.0  0.0   3728  2260 ?        S    Oct25   0:00 /usr/bin/bwrap --args 42 -- brave
```



```
234066656,262144 --disable-features=DesktopPWAsRunOnOsLogin,EyeDropp
er,WebAssemblyTrapHandler --variations-seed-version=main@3f414f362d2
cf54e91175aaf42a3669694fe4d96
jakedav+   22017 42.6  4.4 1461829904 714764 ?   Sl   14:43  42:25 /
app/brave/brave --type=renderer --crashpad-handler-pid=14 --enable-c
rash-reporter=b216ecd6-33f2-43b3-a1f0-233e850dc302, --enable-distill
ability-service --origin-trial-public-key=bYUKPJoPnCxeNvu72j4EmPuK7t
r1PAC7SHh8ld9Mw3E=,fMS4mpO6buLQ/QMd+zJmxzty/VQ6B1EUZqoCU04zoRU= --ch
ange-stack-guard-on-fork=enable --ozone-platform=wayland --lang=en-U
S --num-raster-threads=4 --enable-main-frame-before-activation --ren
derer-client-id=189 --time-ticks-at-unix-epoch=-1761427930079144 --l
aunch-time-ticks=21649454166 --shared-files=v8_context_snapshot_data
:100 --metrics-shmem-handle=4,i,3002689125300677218,8581513587719306
22,2097152 --field-trial-handle=3,i,7698244786761223361,267659651723
4066656,262144 --disable-features=DesktopPWAsRunOnOsLogin,EyeDropper
,WebAssemblyTrapHandler --variations-seed-version=main@3f414f362d2cf
54e91175aaf42a3669694fe4d96
jakedav+   22866 18.5  5.1 1466884832 822720 ?   Sl   14:49  17:15 /
app/brave/brave --type=renderer --crashpad-handler-pid=14 --enable-c
rash-reporter=b216ecd6-33f2-43b3-a1f0-233e850dc302, --enable-distill
ability-service --origin-trial-public-key=bYUKPJoPnCxeNvu72j4EmPuK7t
r1PAC7SHh8ld9Mw3E=,fMS4mpO6buLQ/QMd+zJmxzty/VQ6B1EUZqoCU04zoRU= --ch
ange-stack-guard-on-fork=enable --ozone-platform=wayland --lang=en-U
S --num-raster-threads=4 --enable-main-frame-before-activation --ren
derer-client-id=214 --time-ticks-at-unix-epoch=-1761427930079144 --l
aunch-time-ticks=22028540314 --shared-files=v8_context_snapshot_data
:100 --metrics-shmem-handle=4,i,15277481941362526189,187888727415996
2827,2097152 --field-trial-handle=3,i,7698244786761223361,2676596517
234066656,262144 --disable-features=DesktopPWAsRunOnOsLogin,EyeDropp
er,WebAssemblyTrapHandler --variations-seed-version=main@3f414f362d2
cf54e91175aaf42a3669694fe4d96
jakedav+   24615  0.0  0.4 1459926736 76204 ?    Sl   16:03   0:00 /
app/brave/brave --type=renderer --crashpad-handler-pid=14 --enable-c
rash-reporter=b216ecd6-33f2-43b3-a1f0-233e850dc302, --enable-distill
ability-service --origin-trial-public-key=bYUKPJoPnCxeNvu72j4EmPuK7t
r1PAC7SHh8ld9Mw3E=,fMS4mpO6buLQ/QMd+zJmxzty/VQ6B1EUZqoCU04zoRU= --ch
ange-stack-guard-on-fork=enable --ozone-platform=wayland --lang=en-U
S --num-raster-threads=4 --enable-main-frame-before-activation --ren
derer-client-id=226 --time-ticks-at-unix-epoch=-1761427930079144 --l
aunch-time-ticks=26467514102 --shared-files=v8_context_snapshot_data
:100 --metrics-shmem-handle=4,i,1690464906406662763,1722563069175057
6683,2097152 --field-trial-handle=3,i,7698244786761223361,2676596517
234066656,262144 --disable-features=DesktopPWAsRunOnOsLogin,EyeDropp
er,WebAssemblyTrapHandler --variations-seed-version=main@3f414f362d2
cf54e91175aaf42a3669694fe4d96
jakedav+   25130  0.0  0.0 231252  2536 pts/0    S+   16:22   0:00 g
rep --color=auto brave
jakedavies@fedora:~/htop_soc_project$ _
```



```
dle=4,i,12590979685588624832,9164888262363651600,2097152 --field-trial-handle=3,i,7698
ations-seed-version=main@3f414f362d2cf54e91175aaf42a3669694fe4d96
jakedav+   22017 42.6  4.4 1461829904 714764 ?   Sl   14:43  42:25 /app/brave/brave --
service --origin-trial-public-key=bYUKPJoPnCxeNvu72j4EmPuK7tr1PAC7SHh8ld9Mw3E=,fMS4mpO
hreads=4 --enable-main-frame-before-activation --renderer-client-id=189 --time-ticks-a
dle=4,i,3002689125300677218,858151358771930622,2097152 --field-trial-handle=3,i,769824
ions-seed-version=main@3f414f362d2cf54e91175aaf42a3669694fe4d96
jakedav+   22866 18.5  5.1 1466884832 822720 ?   Sl   14:49  17:15 /app/brave/brave --
service --origin-trial-public-key=bYUKPJoPnCxeNvu72j4EmPuK7tr1PAC7SHh8ld9Mw3E=,fMS4mpO
hreads=4 --enable-main-frame-before-activation --renderer-client-id=214 --time-ticks-a
dle=4,i,15277481941362526189,1878887274159962827,2097152 --field-trial-handle=3,i,7698
```

As we can see under the PID's 22017 & 22866 There are two high CPU's reading at 42.6 & 18.5

Overview

Simulated a SOC alert for high CPU usage using `htop` on Fedora 42, mimicking malware triage for Evalian’s L1 role.

Step 1: Setup

Created folder with `mkdir ~/htop_soc_project` and navigated with `cd`.

Step 2: Monitor Processes

Used `htop`, sorted by CPU (`F6`), filtered `firefox` (`F4`), paused (`F2`).

Step 3: Escalate

Created ticket with `echo` to `htop_alert.txt`.

Step 4 (Optional): Cross-Check

Used `ps aux | grep brave` to confirm.

Tie to SOC

Shows I can monitor systems with `htop` and escalate anomalies, per Evalian’s requirements. Links to Cyber Kill Chain’s Exploitation stage (malware).