ASSESSMENT -1

Animikha Sinha | Cyber Security and Ethical Hacking

File and Directory Operations

1. ls: List files and directories

```
animikha@LAPTOP-PUGUNFUJ: ~
animikha@LAPTOP-PUGUNFUJ:~$ ls
A1Q2.c      A3Q1.c      Megumi          a.txt         child7.c          first                matMul2.c          pthreadsMonCat.c      temp_alert
A1Q3.c      A3Q2.c      Pipes.c         addition.cpp  child8.c          haruno.c             matMul3.c          raceCond.c            temp_sms.py
A1Q4        A3Q3.c      Pipes_2.c       bin           crc.c             hello.py             matMul4.c          raymondTree.cpp       temp_sms.py.save
A1Q4.c      A4Q1.cpp    Pthreads_1.c    bullyAlgo.c   device_control.py ic-projects          node_modules       ringAlgo.c            test
A2Q1.c      A4Q2.cpp    Shared_memo_1.c caz.c         device_status.py  itadori              ompFibo.c          sakura.c              twilo_conf.py
A2Q1_hcf    ANIMIKHA    Shared_memory.c caz3.c        dotProduct.c      lamBake.c            p-c_sema_071021.c  semaphores_071021.c   vectorAdd.c
A2Q1_hcf.c  CAT_1.c     SumMonCat       child2        ex1.c             lamp2.c              package-lock.json  shm_write.c           vegetables
A2Q1_lcm    FAT_A.c++   SumMonCat.c     child3.c      execlp.c          lamportAlgo.c        package.json       suzuKasaAlgo.c
A2Q1_lcm.c  FAT_B.c     Yuji            child4.c      execlpMonCat.c    led_control.py       pipes.c            suzuKasaAlgo.cpp
A2Q2.c      Fushiguro   __pycache__     child5.c      fcfsMonCat.c      lucky_number_generator.py pr_090921.c  suzuKasaAlgo.cpp.save
A2Q3.c      Itadori     a.out           child6.c      fcfs_020921.c     matMul.c             prct.cpp           taxt
animikha@LAPTOP-PUGUNFUJ:~$
```

2. cd: Change directory

Changing from home to root directory

```
animikha@LAPTOP-PUGUNFUJ:~$ cd /
animikha@LAPTOP-PUGUNFUJ:/$
```

3. **pwd: Prints current working directory**

```
animikha@LAPTOP-PUGUNFUJ:~$ cd /
animikha@LAPTOP-PUGUNFUJ:/$ pwd
/
```

4. **mkdir: Make directory**

```
animikha@LAPTOP-PUGUNFUJ:~$ mkdir CyberSecurity
animikha@LAPTOP-PUGUNFUJ:~$ ls
A1Q2.c      A3Q1.c         Itadori          a.out         child6.c          fcfs_020921.c             matMul.c          prct.cpp              taxt
A1Q3.c      A3Q2.c         Megumi           a.txt         child7.c          first                     matMul2.c         pthreadsMonCat.c      temp_alert
A1Q4        A3Q3.c         Pipes.c          addition.cpp  child8.c          haruno.c                  matMul3.c         raceCond.c            temp_sms.py
A1Q4.c      A4Q1.cpp       Pipes_2.c        bin           crc.c             hello.py                  matMul4.c         raymondTree.cpp       temp_sms.py.save
A2Q1.c      A4Q2.cpp       Pthreads_1.c     bullyAlgo.c   device_control.py ic-projects               node_modules      ringAlgo.c            test
A2Q1_hcf    ANIMIKHA       Shared_memo_1.c  caz.c         device_status.py  itadori                   ompFibo.c         sakura.c              twilo_conf.py
A2Q1_hcf.c  CAT_1.c        Shared_memory.c  caz3.c        dotProduct.c      lamBake.c                 p-c_sema_071021.c semaphores_071021.c   vectorAdd.c
A2Q1_lcm    CyberSecurity  SumMonCat        child2        ex1.c             lamp2.c                   package-lock.json shm_write.c           vegetables
A2Q1_lcm.c  FAT_A.c++      SumMonCat.c      child3.c      execlp.c          lamportAlgo.c             package.json      suzuKasaAlgo.c
A2Q2.c      FAT_B.c        Yuji             child4.c      execlpMonCat.c    led_control.py            pipes.c           suzuKasaAlgo.cpp
A2Q3.c      Fushiguro      __pycache__      child5.c      fcfsMonCat.c      lucky_number_generator.py pr_090921.c       suzuKasaAlgo.cpp.save
animikha@LAPTOP-PUGUNFUJ:~$
```

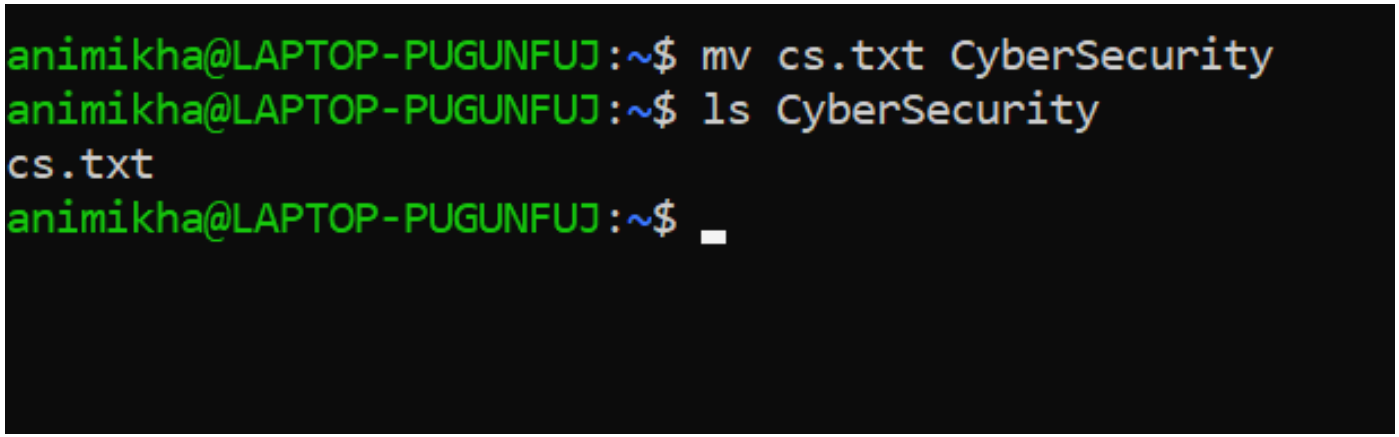
5. touch: Create an empty file

```
animikha@LAPTOP-PUGUNFUJ:~$ touch emptyFile.txt
animikha@LAPTOP-PUGUNFUJ:~$ cat emptyFile.txt
animikha@LAPTOP-PUGUNFUJ:~$
```

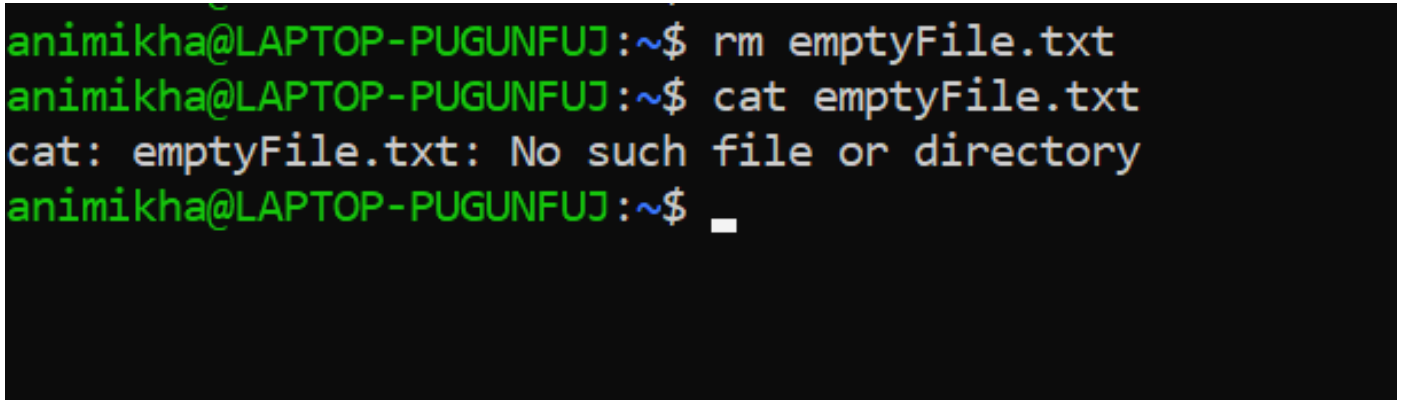
6. cp: Copy files and directories

```
animikha@LAPTOP-PUGUNFUJ:~$ cat cs.txt
I am a Security Analyst

animikha@LAPTOP-PUGUNFUJ:~$ cp cs.txt emptyFile.txt
animikha@LAPTOP-PUGUNFUJ:~$ cat emptyFile.txt
I am a Security Analyst

animikha@LAPTOP-PUGUNFUJ:~$
```

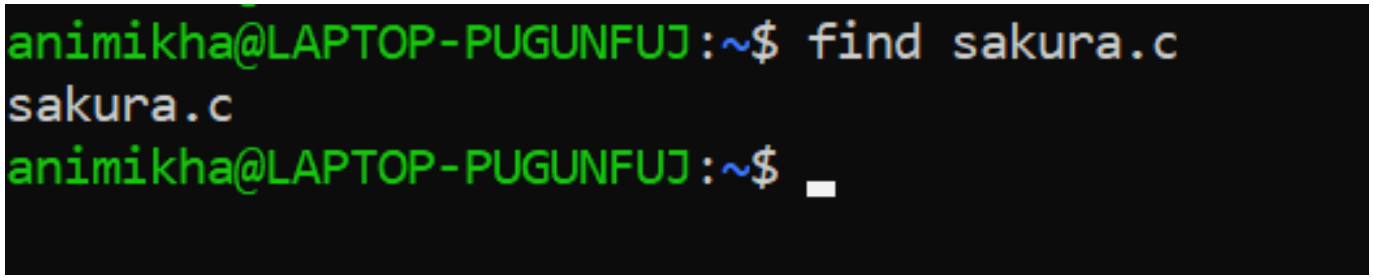
7. mv: Move or rename files and directories



8. rm: Remove files and directories



9. find: Search for files and directories



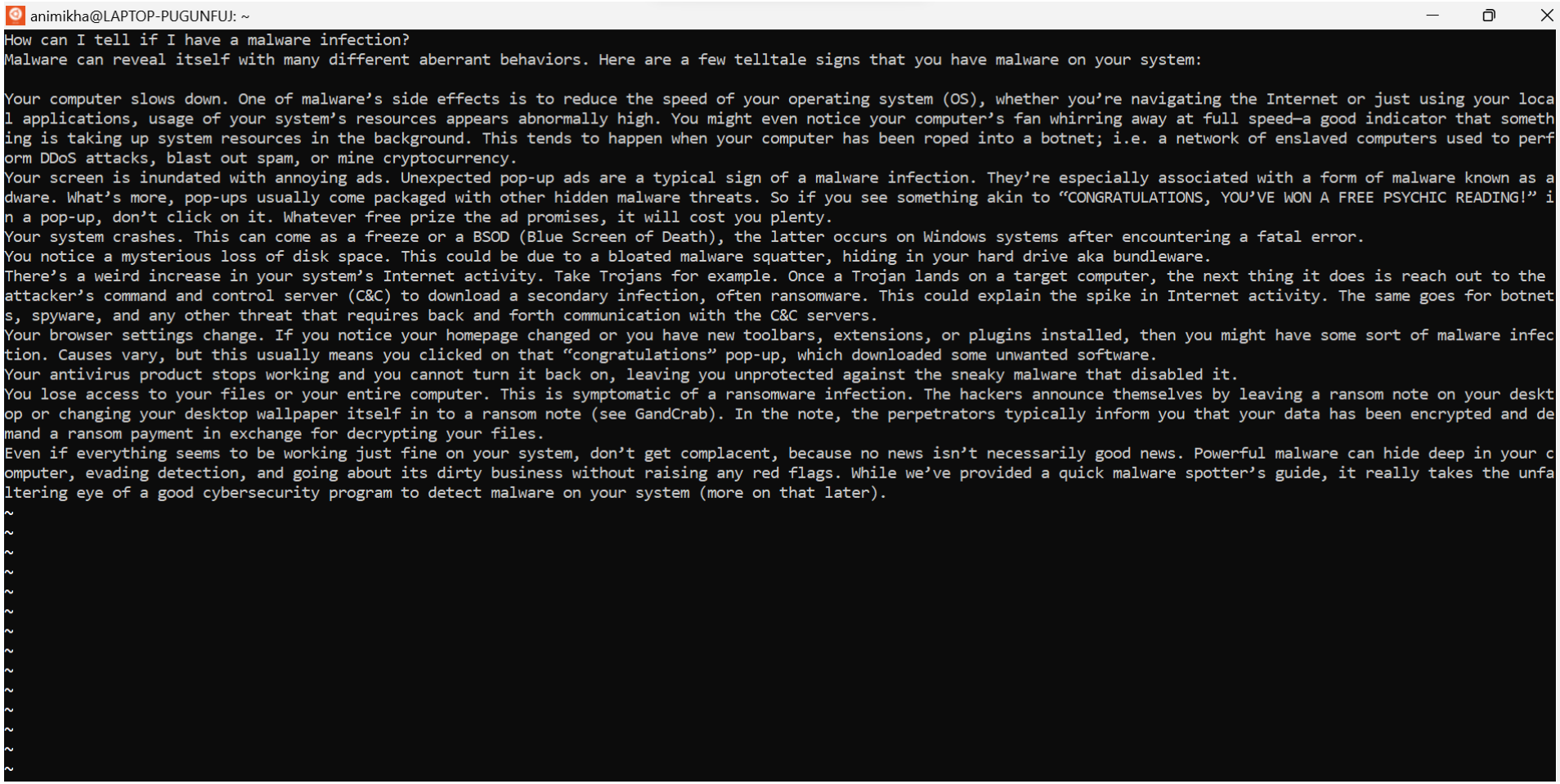
File Viewing and Editing

1. **cat: Concatenate and display file content**

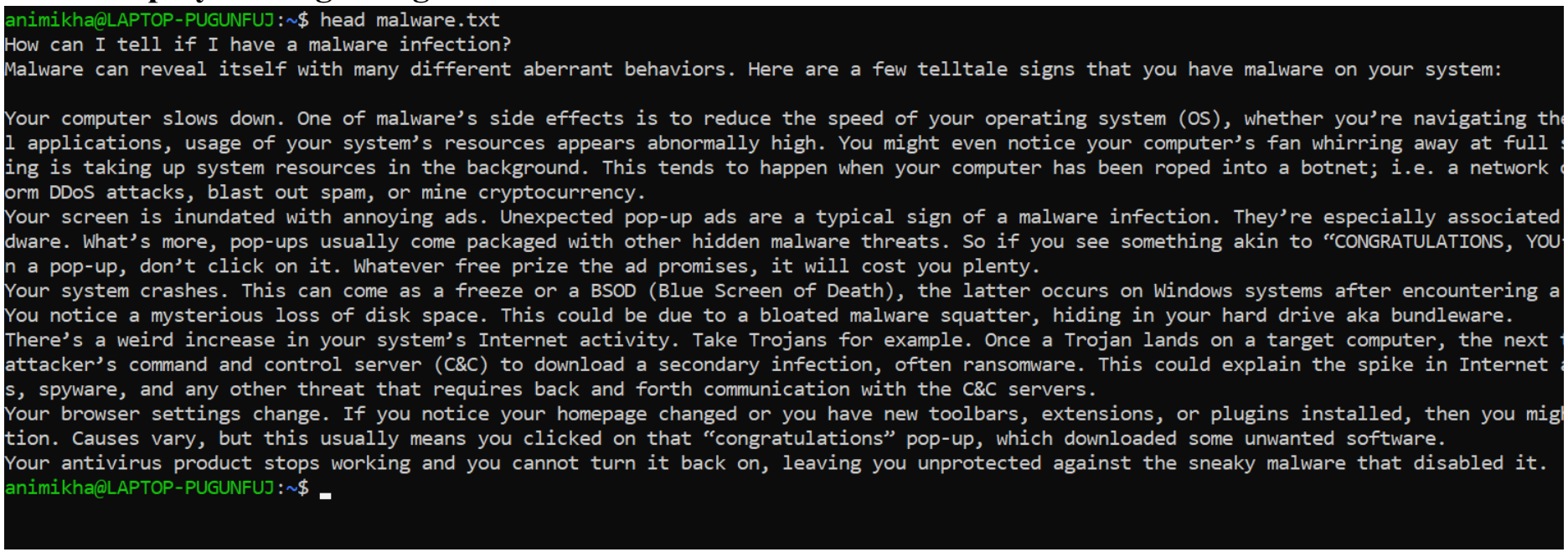
```
animikha@LAPTOP-PUGUNFUJ:~$ cat sakura.c
#include<stdio.h>
int main()
{
        printf("Hello\n");
}
animikha@LAPTOP-PUGUNFUJ:~$
```

2. less: View file content with pagination

The less command is a Linux terminal pager that shows a file's contents one screen at a time. It is useful when dealing with a large text file because it doesn't load the entire file but accesses it page by page, resulting in fast loading speeds



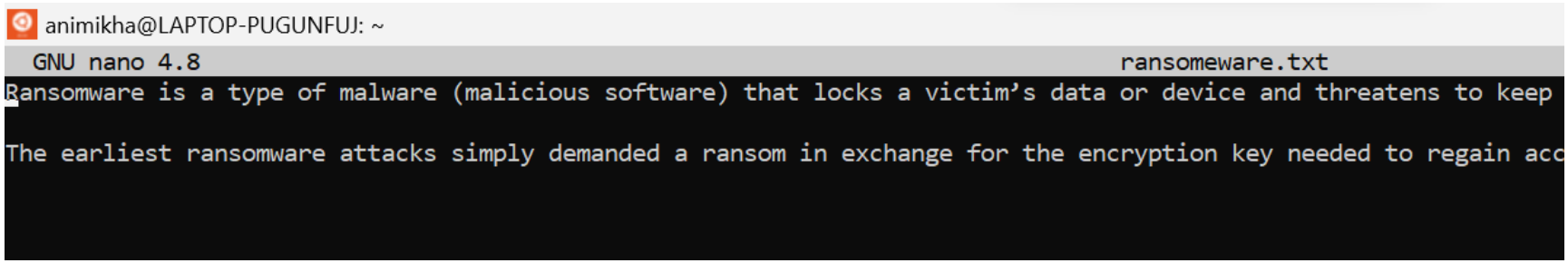
3. head: Display the beginning of a file

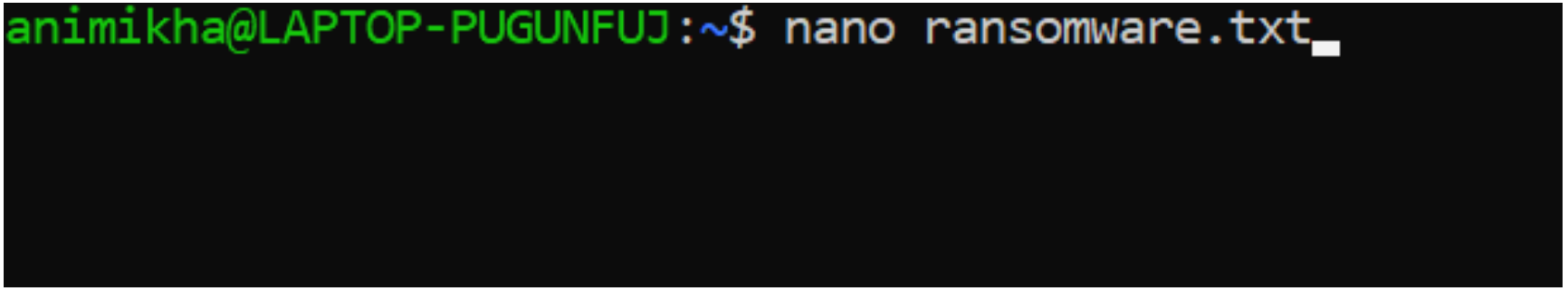


4. tail: Display the end of a file

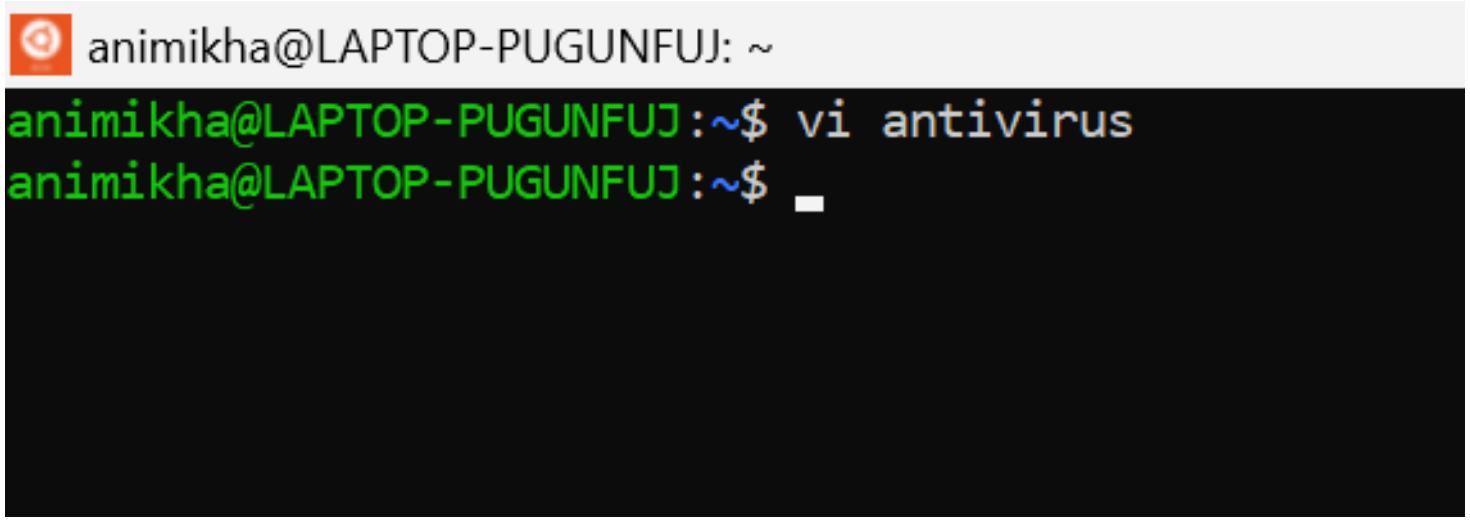
```
animikha@LAPTOP-PUGUNFUJ:~$ tail malware.txt

Your computer slows down. One of malware's side effects is to reduce the speed of your operating system (OS), whether you're navigat
l applications, usage of your system's resources appears abnormally high. You might even notice your computer's fan whirring away at
ing is taking up system resources in the background. This tends to happen when your computer has been roped into a botnet; i.e. a ne
orm DDoS attacks, blast out spam, or mine cryptocurrency.
Your screen is inundated with annoying ads. Unexpected pop-up ads are a typical sign of a malware infection. They're especially assc
dware. What's more, pop-ups usually come packaged with other hidden malware threats. So if you see something akin to "CONGRATULATION
n a pop-up, don't click on it. Whatever free prize the ad promises, it will cost you plenty.
Your system crashes. This can come as a freeze or a BSOD (Blue Screen of Death), the latter occurs on Windows systems after encounte
You notice a mysterious loss of disk space. This could be due to a bloated malware squatter, hiding in your hard drive aka bundlewar
There's a weird increase in your system's Internet activity. Take Trojans for example. Once a Trojan lands on a target computer, the
attacker's command and control server (C&C) to download a secondary infection, often ransomware. This could explain the spike in Int
s, spyware, and any other threat that requires back and forth communication with the C&C servers.
Your browser settings change. If you notice your homepage changed or you have new toolbars, extensions, or plugins installed, then y
tion. Causes vary, but this usually means you clicked on that "congratulations" pop-up, which downloaded some unwanted software.
Your antivirus product stops working and you cannot turn it back on, leaving you unprotected against the sneaky malware that disable
You lose access to your files or your entire computer. This is symptomatic of a ransomware infection. The hackers announce themselve
op or changing your desktop wallpaper itself in to a ransom note (see GandCrab). In the note, the perpetrators typically inform you
mand a ransom payment in exchange for decrypting your files.
Even if everything seems to be working just fine on your system, don't get complacent, because no news isn't necessarily good news.
omputer, evading detection, and going about its dirty business without raising any red flags. While we've provided a quick malware s
ltering eye of a good cybersecurity program to detect malware on your system (more on that later).
animikha@LAPTOP-PUGUNFUJ:~$
```

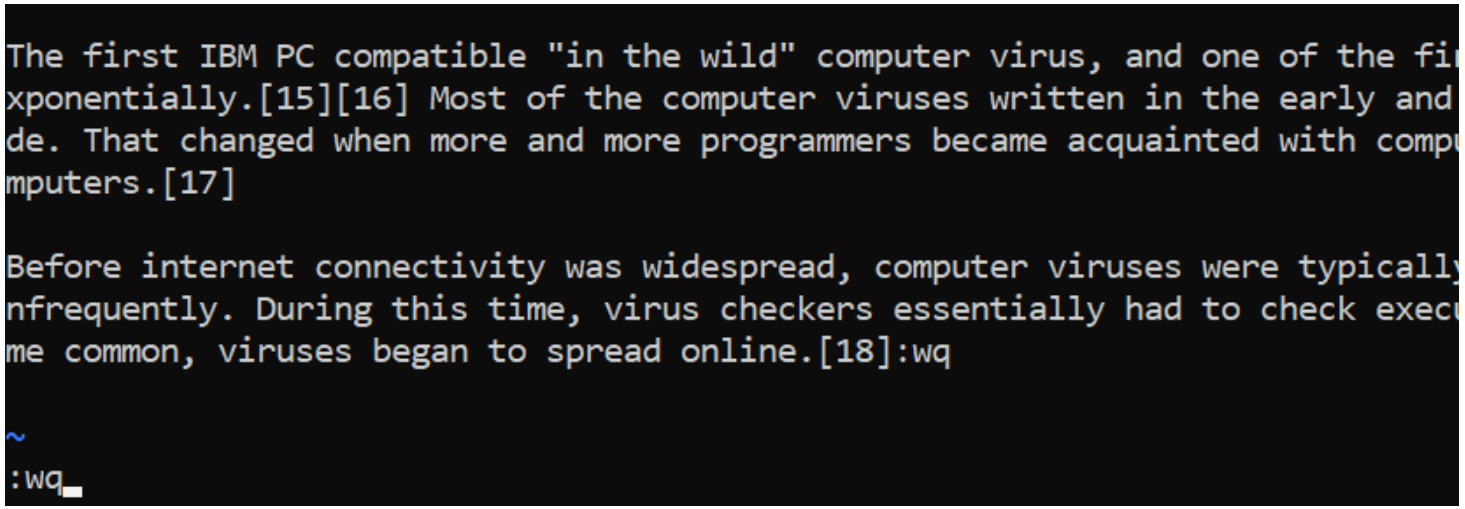
5. nano: Text editor for creating and editing files





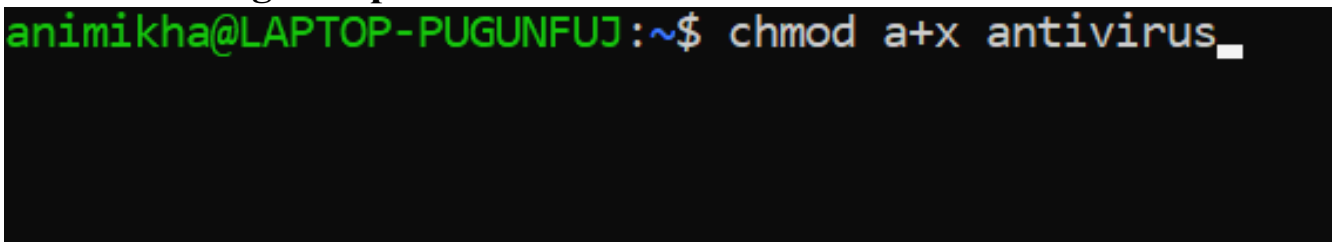
6. **vi/vim: Powerful text editor for experienced users**



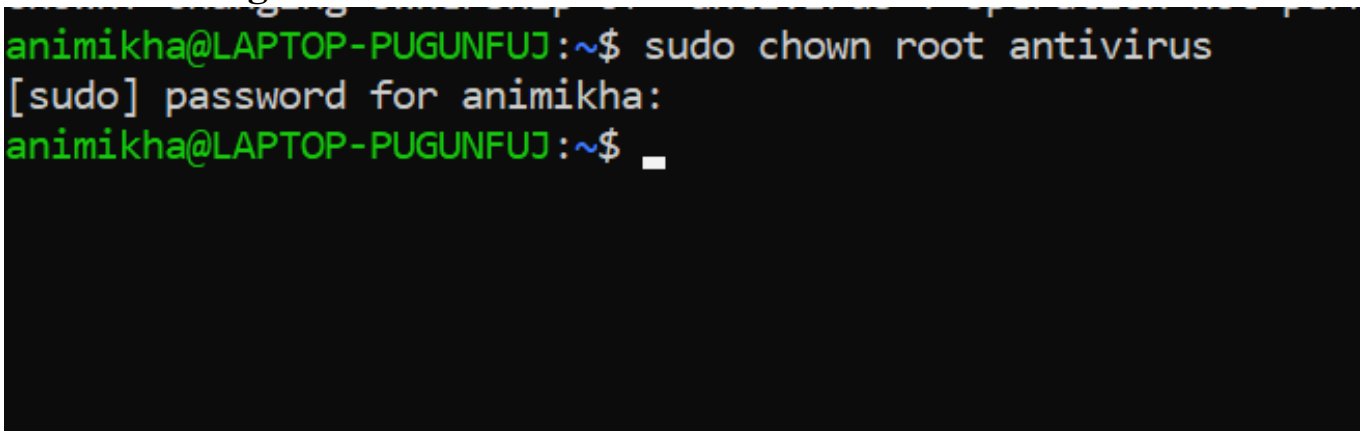


File Permissions

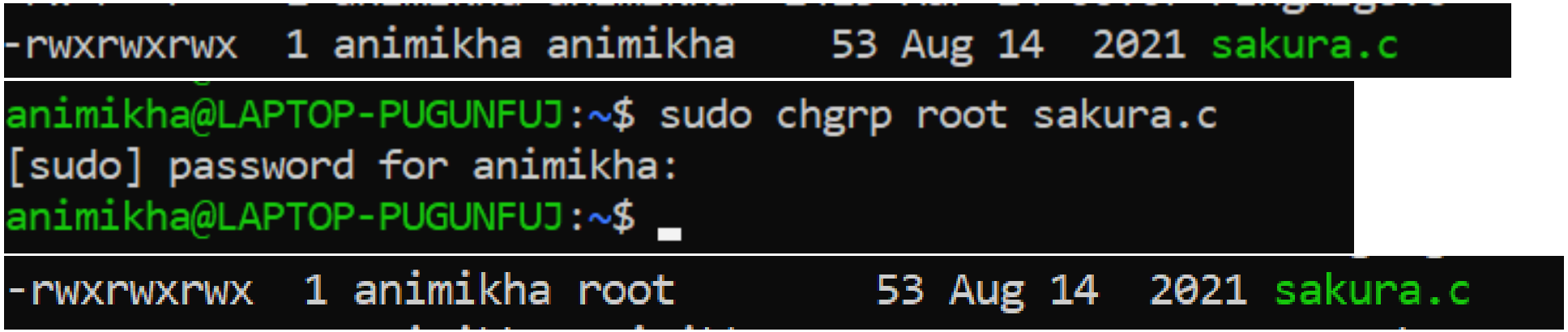
1. **chmod: Change file permissions**



2. **chown: Change file owner**



3. chgrp: Change file group



File Compression and Archiving

1. **tar: Archive files**

```
animikha@LAPTOP-PUGUNFUJ:~$ tar cvf file.tar *.c
A1Q2.c
A1Q3.c
A1Q4.c
A2Q1.c
A2Q1_hcf.c
A2Q1_lcm.c
A2Q2.c
A2Q3.c
A3Q1.c
A3Q2.c
A3Q3.c
CAT_1.c
FAT_B.c
Pipes.c
Pipes_2.c
Pthreads_1.c
Shared_memo_1.c
Shared_memory.c
SumMonCat.c
bullyAlgo.c
caz.c
caz3.c
child3.c
child4.c
child5.c
child6.c
child7.c
child8.c
```

2. **gzip: Compress files**

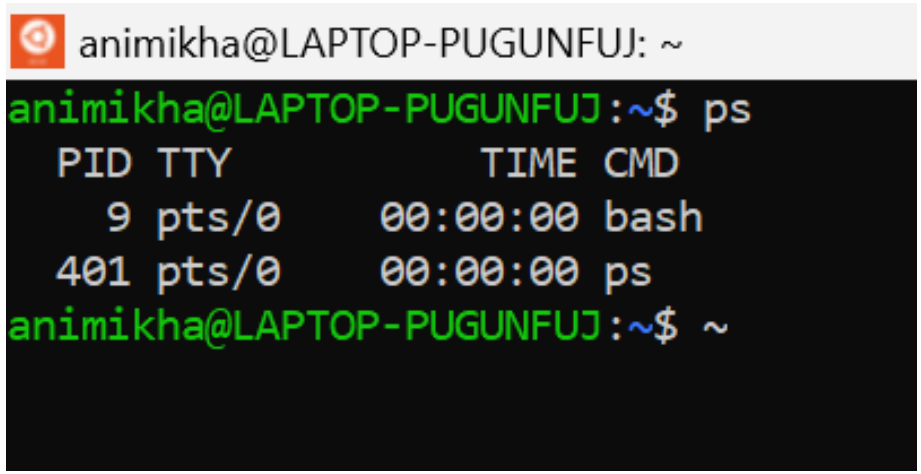
```
animikha@LAPTOP-PUGUNFUJ:~$ gzip -f child3.c
animikha@LAPTOP-PUGUNFUJ:~$ gzip -L child3.gz
gzip 1.10
Copyright (C) 2018 Free Software Foundation, Inc.
Copyright (C) 1993 Jean-loup Gailly.
This is free software.  You may redistribute copies of it under the terms of
the GNU General Public License <https://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.
animikha@LAPTOP-PUGUNFUJ:~$
```

3. **unzip: Extract files from a ZIP archive**

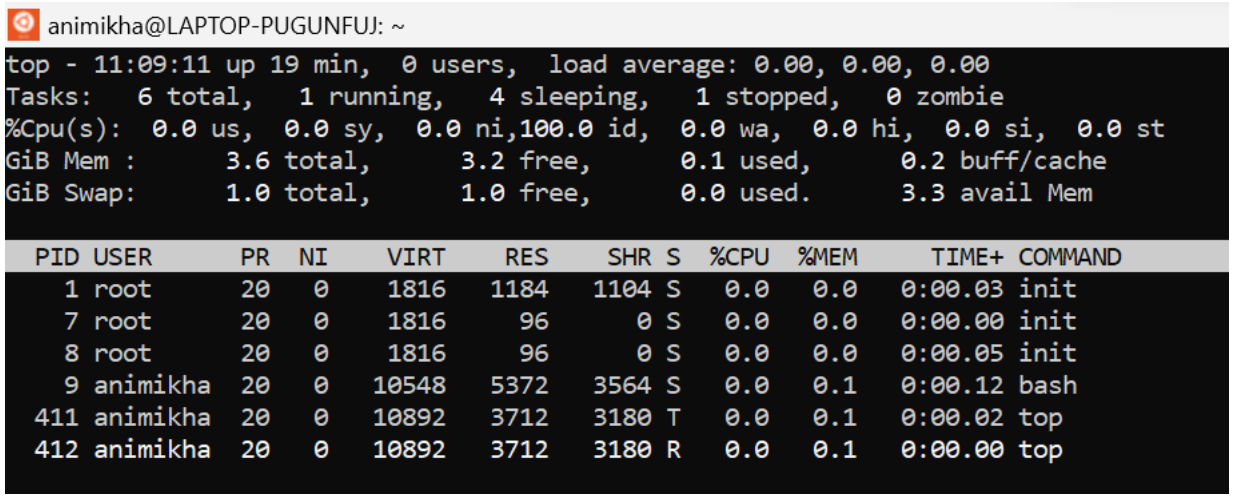
```
animikha@LAPTOP-PUGUNFUJ:~$ unzip '*.zip'
unzip:  cannot find or open *.zip, *.zip.zip or *.zip.ZIP.

No zipfiles found.
animikha@LAPTOP-PUGUNFUJ:~$
```

Process Management

1. **ps: List running processes**



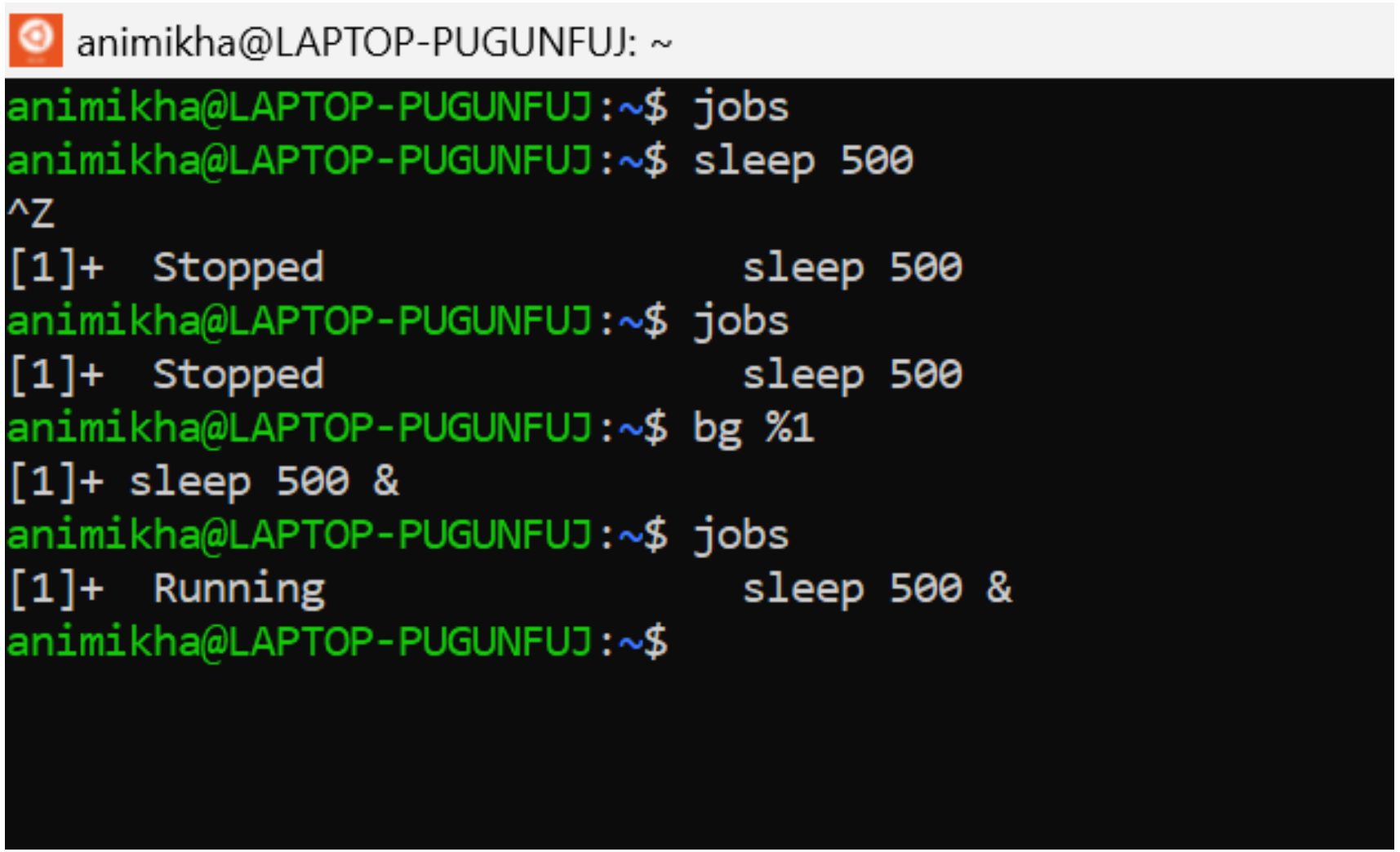
2. **top: Display real-time system information and processes**



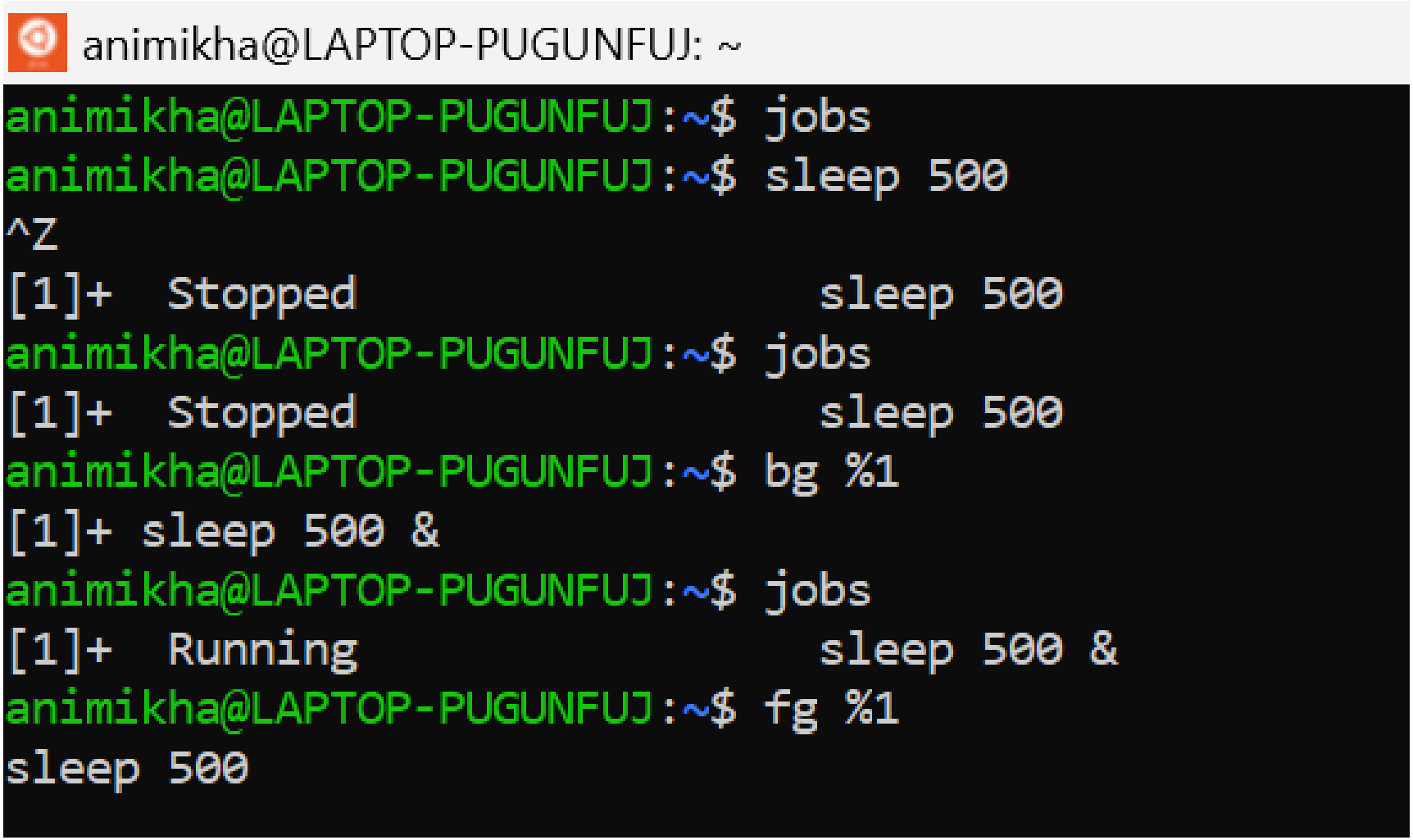
3. **kill: Terminate processes**

```
animikha@LAPTOP-PUGUNFUJ:~$ kill -l
 1) SIGHUP       2) SIGINT       3) SIGQUIT      4) SIGILL       5) SIGTRAP
 6) SIGABRT      7) SIGBUS       8) SIGFPE       9) SIGKILL     10) SIGUSR1
11) SIGSEGV     12) SIGUSR2     13) SIGPIPE     14) SIGALRM     15) SIGTERM
16) SIGSTKFLT   17) SIGCHLD     18) SIGCONT     19) SIGSTOP     20) SIGTSTP
21) SIGTTIN     22) SIGTTOU     23) SIGURG      24) SIGXCPU     25) SIGXFSZ
26) SIGVTALRM   27) SIGPROF     28) SIGWINCH    29) SIGIO       30) SIGPWR
31) SIGSYS      34) SIGRTMIN    35) SIGRTMIN+1  36) SIGRTMIN+2  37) SIGRTMIN+3
38) SIGRTMIN+4  39) SIGRTMIN+5  40) SIGRTMIN+6  41) SIGRTMIN+7  42) SIGRTMIN+8
43) SIGRTMIN+9  44) SIGRTMIN+10 45) SIGRTMIN+11 46) SIGRTMIN+12 47) SIGRTMIN+13
48) SIGRTMIN+14 49) SIGRTMIN+15 50) SIGRTMAX-14 51) SIGRTMAX-13 52) SIGRTMAX-12
53) SIGRTMAX-11 54) SIGRTMAX-10 55) SIGRTMAX-9  56) SIGRTMAX-8  57) SIGRTMAX-7
58) SIGRTMAX-6  59) SIGRTMAX-5  60) SIGRTMAX-4  61) SIGRTMAX-3  62) SIGRTMAX-2
63) SIGRTMAX-1  64) SIGRTMAX
animikha@LAPTOP-PUGUNFUJ:~$ kill 411
```

4. **bg: Run processes in the background**

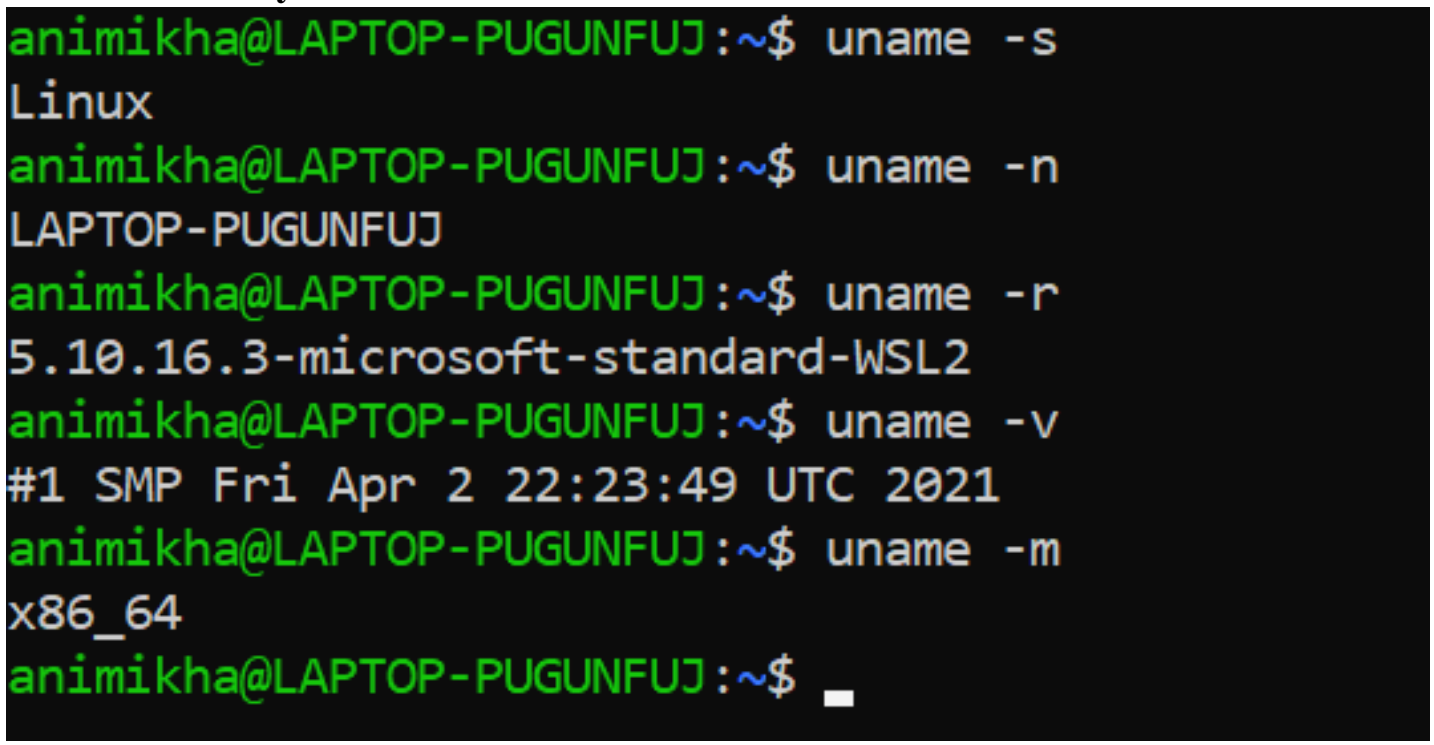


5. **fg: Bring background processes to the foreground**



System Information

1. **uname: Print system information**



2. df: Display disk space usage

```
animikha@LAPTOP-PUGUNFUJ:~$ df
Filesystem     1K-blocks      Used Available Use% Mounted on
/dev/sdb       263174212   6914056 242822000   3% /
tools          224090436 181433208  42657228  81% /init
none             1859384         0   1859384   0% /dev
tmpfs            1861468         0   1861468   0% /sys/fs/cgroup
none             1861468         4   1861464   1% /run
none             1861468         0   1861468   0% /run/lock
none             1861468         0   1861468   0% /run/shm
none             1861468         0   1861468   0% /run/user
drivers        224090436 181433208  42657228  81% /usr/lib/wsl/drivers
lib            224090436 181433208  42657228  81% /usr/lib/wsl/lib
none             1861468         4   1861464   1% /mnt/wsl
drvfsa         224090436 181433208  42657228  81% /mnt/c
drvfsa         152765436 118675832  34089604  78% /mnt/d
drvfsa          52032508   6141164  45891344  12% /mnt/e
drvfsa          51199996  47296232   3903764  93% /mnt/f
animikha@LAPTOP-PUGUNFUJ:~$
```

3. free: Display memory usage

```
animikha@LAPTOP-PUGUNFUJ:~$ free
               total        used        free      shared  buff/cache   available
Mem:         3722936      106720     3384324          72      231892     3465748
Swap:        1048576           0     1048576
animikha@LAPTOP-PUGUNFUJ:~$
```

4. **uptime: Show system uptime**

```
animikha@LAPTOP-PUGUNFUJ:~$ uptime
 15:20:26 up  3:13,  0 users,  load average: 0.00, 0.00, 0.00
animikha@LAPTOP-PUGUNFUJ:~$
```

5. **who: Display logged-in users**

```
animikha@LAPTOP-PUGUNFUJ:~$ who -m -H
NAME     LINE         TIME             COMMENT
animikha@LAPTOP-PUGUNFUJ:~$ who -T -H
NAME       LINE         TIME             COMMENT
animikha@LAPTOP-PUGUNFUJ:~$ who -u
animikha@LAPTOP-PUGUNFUJ:~$
```

6. **w: Display logged-in users and their activities**

```
animikha@LAPTOP-PUGUNFUJ:~$ w
 15:28:48 up  3:21,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
animikha@LAPTOP-PUGUNFUJ:~$ w -u
 15:29:46 up  3:22,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
animikha@LAPTOP-PUGUNFUJ:~$ w -s
 15:29:51 up  3:22,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              IDLE WHAT
animikha@LAPTOP-PUGUNFUJ:~$
```

Networking

1. ifconfig: Configure network interfaces

```
animikha@LAPTOP-PUGUNFUJ:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.27.86.226  netmask 255.255.240.0  broadcast 172.27.95.255
        inet6 fe80::215:5dff:fe6f:3fd3  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:6f:3f:d3  txqueuelen 1000  (Ethernet)
        RX packets 1954  bytes 513389 (513.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 118  bytes 8200 (8.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

animikha@LAPTOP-PUGUNFUJ:~$
```

2. ping: Send ICMP echo requests to a network host

```
animikha@LAPTOP-PUGUNFUJ:~$ ping -c 5 www.geeksforgeeks.org
PING a1991.dscr.akamai.net (203.171.247.211) 56(84) bytes of data.
64 bytes from node-203-171-247-211.alliancebroadband.in (203.171.247.211): icmp_seq=1 ttl=59 time=3.80 ms
64 bytes from node-203-171-247-211.alliancebroadband.in (203.171.247.211): icmp_seq=2 ttl=59 time=7.42 ms
64 bytes from node-203-171-247-211.alliancebroadband.in (203.171.247.211): icmp_seq=3 ttl=59 time=5.78 ms
64 bytes from node-203-171-247-211.alliancebroadband.in (203.171.247.211): icmp_seq=4 ttl=59 time=6.12 ms
64 bytes from node-203-171-247-211.alliancebroadband.in (203.171.247.211): icmp_seq=5 ttl=59 time=5.73 ms

--- a1991.dscr.akamai.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 3.804/5.769/7.416/1.157 ms
```

3. wget: Download files from the web

```
animikha@LAPTOP-PUGUNFUJ:~$ wget http://info.cern.ch/
--2023-05-28 15:48:07--  http://info.cern.ch/
Resolving info.cern.ch (info.cern.ch)... 188.184.21.108, 2001:1458:d00:34::100:125
Connecting to info.cern.ch (info.cern.ch)|188.184.21.108|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 646 [text/html]
Saving to: ‘index.html’

index.html                          100%[=======================================================================================>]     646  --.-KB/s    in 0s

2023-05-28 15:48:08 (6.27 MB/s) - ‘index.html’ saved [646/646]
```

System Administration

1. **sudo: Execute commands with superuser privileges**

```
animikha@LAPTOP-PUGUNFUJ:~$ sudo -V
Sudo version 1.8.31
Sudoers policy plugin version 1.8.31
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.31
animikha@LAPTOP-PUGUNFUJ:~$
```

2. **apt-get: Package management for Debian-based distributions**

```
animikha@LAPTOP-PUGUNFUJ:~$ sudo apt-get check
[sudo] password for animikha:
Sorry, try again.
[sudo] password for animikha:
Reading package lists... Done
Building dependency tree
Reading state information... Done
animikha@LAPTOP-PUGUNFUJ:~$
```

3. **systemctl: Manage system services**

```
animikha@LAPTOP-PUGUNFUJ:~$ sudo systemctl mask mysqld
Created symlink /etc/systemd/system/mysqld.service → /dev/null.
animikha@LAPTOP-PUGUNFUJ:~$ sudo systemctl unmask mysqld
Removed /etc/systemd/system/mysqld.service.
animikha@LAPTOP-PUGUNFUJ:~$
```

4. **crontab: Schedule recurring tasks**

```
animikha@LAPTOP-PUGUNFUJ:~$ crontab -u animikha -l
no crontab for animikha
animikha@LAPTOP-PUGUNFUJ:~$ crontab -l
no crontab for animikha
animikha@LAPTOP-PUGUNFUJ:~$
```

5. **useradd: Add a new user**

```
animikha@LAPTOP-PUGUNFUJ:~$ useradd Kitty
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
animikha@LAPTOP-PUGUNFUJ:~$
animikha@LAPTOP-PUGUNFUJ:~$ sudo useradd Kitty
animikha@LAPTOP-PUGUNFUJ:~$
```

6. **passwd: Change user password**

```
animikha@LAPTOP-PUGUNFUJ:~$ sudo useradd Kitty
animikha@LAPTOP-PUGUNFUJ:~$
animikha@LAPTOP-PUGUNFUJ:~$ passwd
Changing password for animikha.
Current password:
New password:
Retype new password:
Password unchanged
```