Fatima Jinnah Women University

Opening Portals of Excellence Through Higher Education

Cloud Computing BSE-VB

Submitted By

Tooba Shafique (2023-BSE-065)

Submitted to

Sir Shoaib

LAB-04

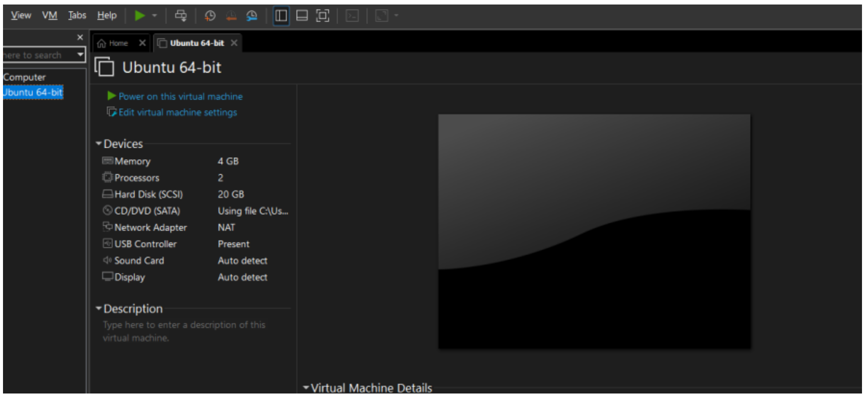
Task 1 – Verify VM Resources in VMware

Step 1: Open VMware Workstation and locate the Ubuntu Server VM used in Lab 1.

Step 2: Inspect the VM settings and note the following details:

- VM Name
- RAM
- CPU
- Disk
- Network Adapter Type

Screenshot: vm_settings.png



Ubuntu 64-bit

Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file C:\Us...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Type here to enter a description of this virtual machine.

Task 2 – Start VM and Log In (Use Your Preferred Host Terminal Method Only)

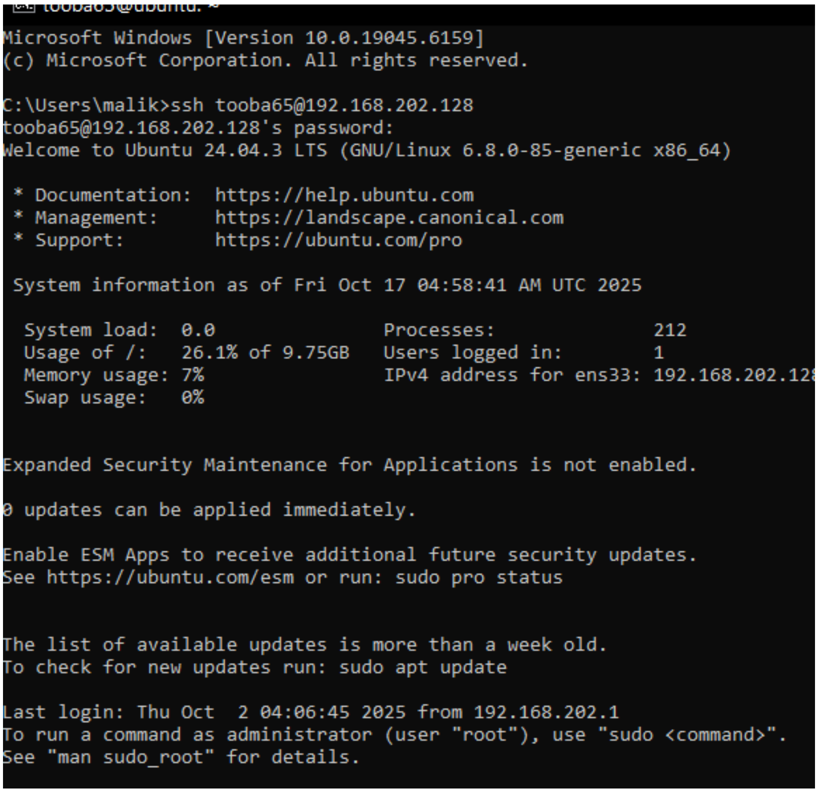
Step 1: Start or resume the VM in VMware Workstation on your host system.

Step 2: Open your preferred terminal on the host (e.g., Command Prompt, PowerShell, macOS Terminal, or Linux Terminal).

Step 3: Connect to the VM using SSH.

Step 4: After connecting, capture a screenshot showing the SSH login prompt or connection result.
Screenshot: vm_login.png

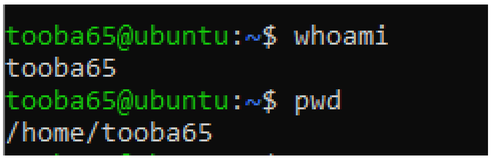
ssh tooba65@192.168.202.128



```
icrosoft Windows [Version 10.0.19045.6159]
(c) Microsoft Corporation. All rights reserved.

C:\Users\malik>ssh tooba65@192.168.202.128
tooba65@192.168.202.128's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-85-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri Oct 17 04:58:41 AM UTC 2025

  System load:  0.0               Processes:             212
  Usage of /:   26.1% of 9.75GB   Users logged in:       1
  Memory usage: 7%                IPv4 address for ens33: 192.168.202.12
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu Oct  2 04:06:45 2025 from 192.168.202.1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Step 5: Run both commands — whoami and pwd — in the same terminal window.

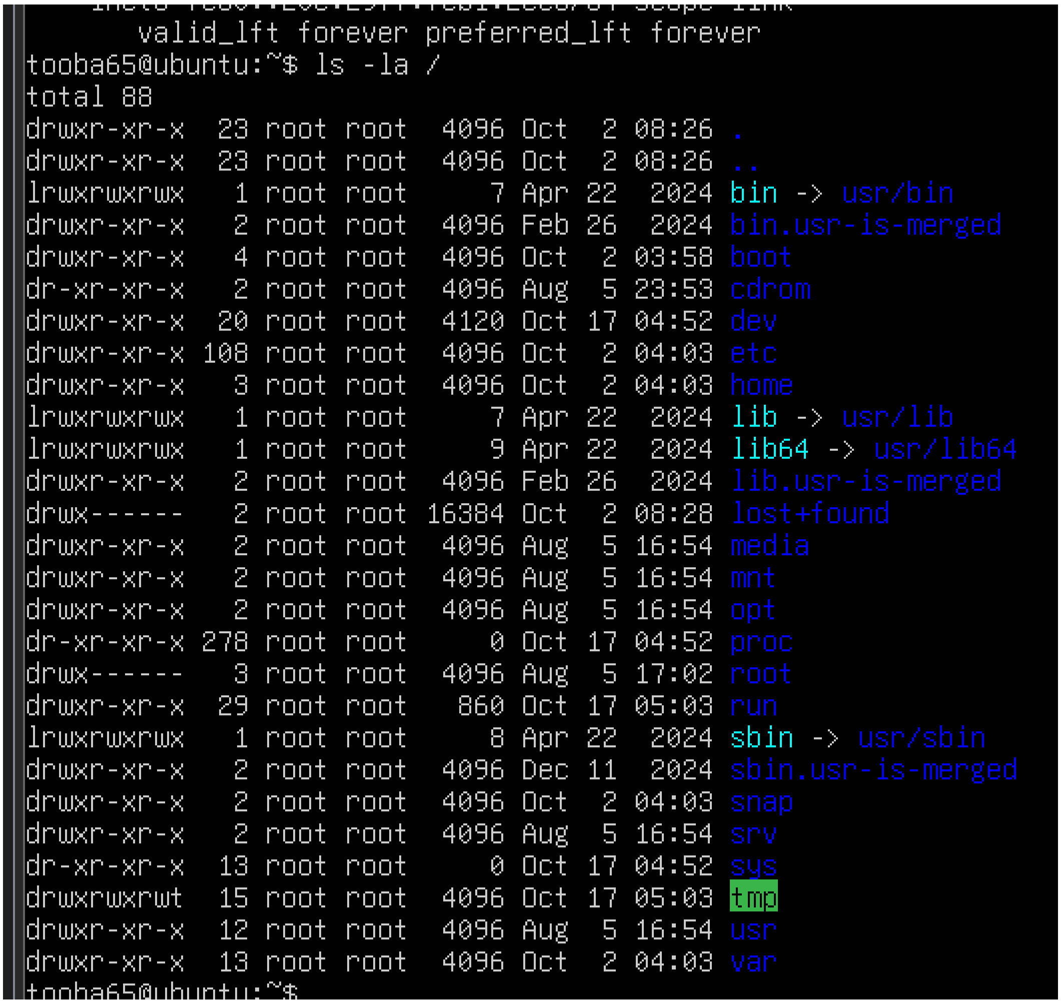
Step 6: Capture a single screenshot showing the outputs of both commands.
Screenshot: whoami_pwd.png



```
tooba65@ubuntu:~$ whoami
tooba65
tooba65@ubuntu:~$ pwd
/home/tooba65
```

Task 3 – Filesystem Exploration — Root Tree and Dotfiles

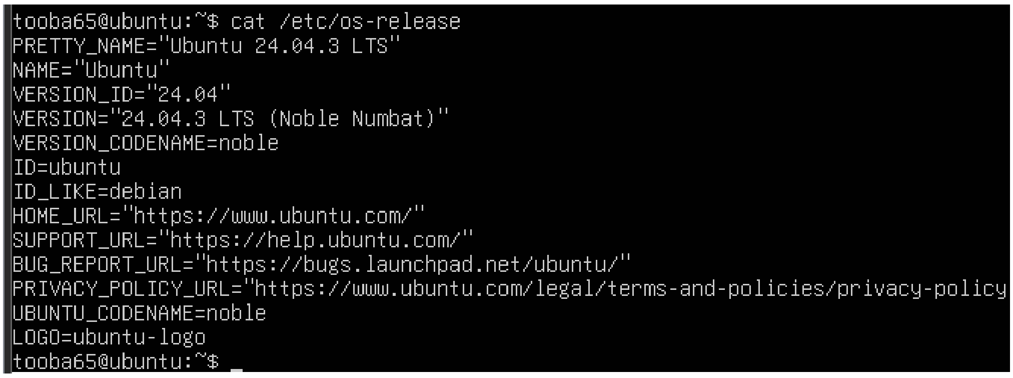
Step 1:



```
      valid_lft forever preferred_lft forever
tooba65@ubuntu:~$ ls -la /
total 88
drwxr-xr-x  23 root root  4096 Oct  2 08:26 .
drwxr-xr-x  23 root root  4096 Oct  2 08:26 ..
lrwxrwxrwx   1 root root     7 Apr 22  2024 bin -> usr/bin
drwxr-xr-x   2 root root  4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x   4 root root  4096 Oct  2 03:58 boot
dr-xr-xr-x   2 root root  4096 Aug  5 23:53 cdrom
drwxr-xr-x  20 root root  4120 Oct 17 04:52 dev
drwxr-xr-x 108 root root  4096 Oct  2 04:03 etc
drwxr-xr-x   3 root root  4096 Oct  2 04:03 home
lrwxrwxrwx   1 root root     7 Apr 22  2024 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Apr 22  2024 lib64 -> usr/lib64
drwxr-xr-x   2 root root  4096 Feb 26  2024 lib.usr-is-merged
drwx------   2 root root 16384 Oct  2 08:28 lost+found
drwxr-xr-x   2 root root  4096 Aug  5 16:54 media
drwxr-xr-x   2 root root  4096 Aug  5 16:54 mnt
drwxr-xr-x   2 root root  4096 Aug  5 16:54 opt
dr-xr-xr-x 278 root root     0 Oct 17 04:52 proc
drwx------   3 root root  4096 Aug  5 17:02 root
drwxr-xr-x  29 root root   860 Oct 17 05:03 run
lrwxrwxrwx   1 root root     8 Apr 22  2024 sbin -> usr/sbin
drwxr-xr-x   2 root root  4096 Dec 11  2024 sbin.usr-is-merged
drwxr-xr-x   2 root root  4096 Oct  2 04:03 snap
drwxr-xr-x   2 root root  4096 Aug  5 16:54 srv
dr-xr-xr-x  13 root root     0 Oct 17 04:52 sys
drwxrwxrwt  15 root root  4096 Oct 17 05:03 tmp
drwxr-xr-x  12 root root  4096 Aug  5 16:54 usr
drwxr-xr-x  13 root root  4096 Oct  2 04:03 var
tooba65@ubuntu:~$
```

Screenshot:

Step 2:
Screenshot: os_release.png

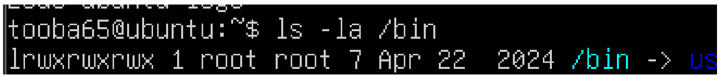


```
tooba65@ubuntu:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
tooba65@ubuntu:~$ _
```

Step 3: Inspect these directories (run each command and screenshot the output):

ls -la /bin

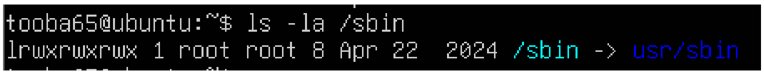
- Save screenshot as ls_bin.png



```
tooba65@ubuntu:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> us
```

ls -la /sbin

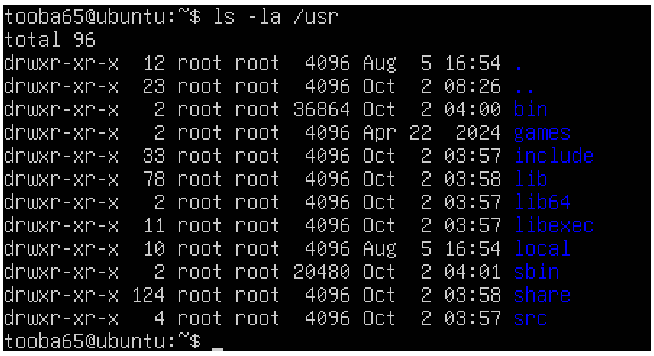
- Save screenshot as ls_sbin.png



```
tooba65@ubuntu:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
```

ls -la /usr

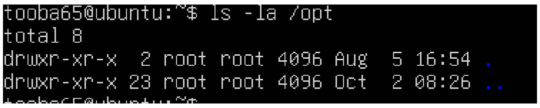
- Save screenshot as ls_usr.png



```
tooba65@ubuntu:~$ ls -la /usr
total 96
drwxr-xr-x  12 root root  4096 Aug  5 16:54 .
drwxr-xr-x  23 root root  4096 Oct  2 08:26 ..
drwxr-xr-x   2 root root 36864 Oct  2 04:00 bin
drwxr-xr-x   2 root root  4096 Apr 22  2024 games
drwxr-xr-x  33 root root  4096 Oct  2 03:57 include
drwxr-xr-x  78 root root  4096 Oct  2 03:58 lib
drwxr-xr-x   2 root root  4096 Oct  2 03:57 lib64
drwxr-xr-x  11 root root  4096 Oct  2 03:57 libexec
drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
drwxr-xr-x   2 root root 20480 Oct  2 04:01 sbin
drwxr-xr-x 124 root root  4096 Oct  2 03:58 share
drwxr-xr-x   4 root root  4096 Oct  2 03:57 src
tooba65@ubuntu:~$ _
```

ls -la /opt

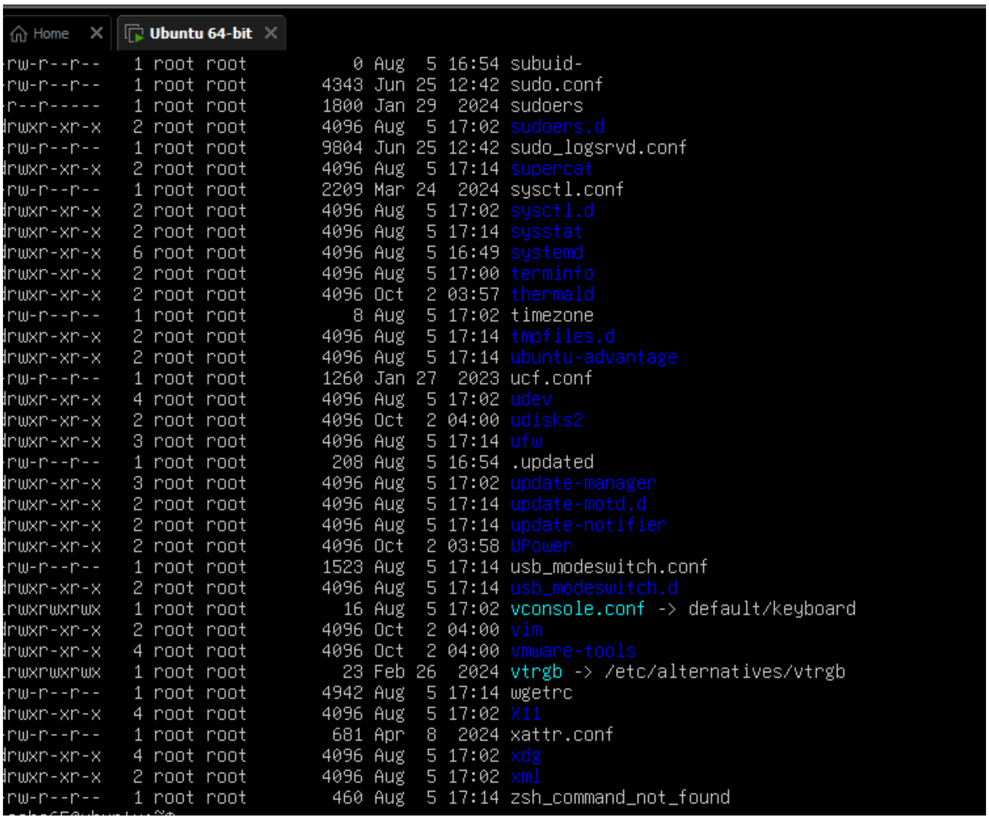
- Save screenshot as ls_opt.png



```
tooba65@ubuntu:~$ ls -la /opt
total 8
drwxr-xr-x  2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Oct  2 08:26 ..
```

ls -la /etc

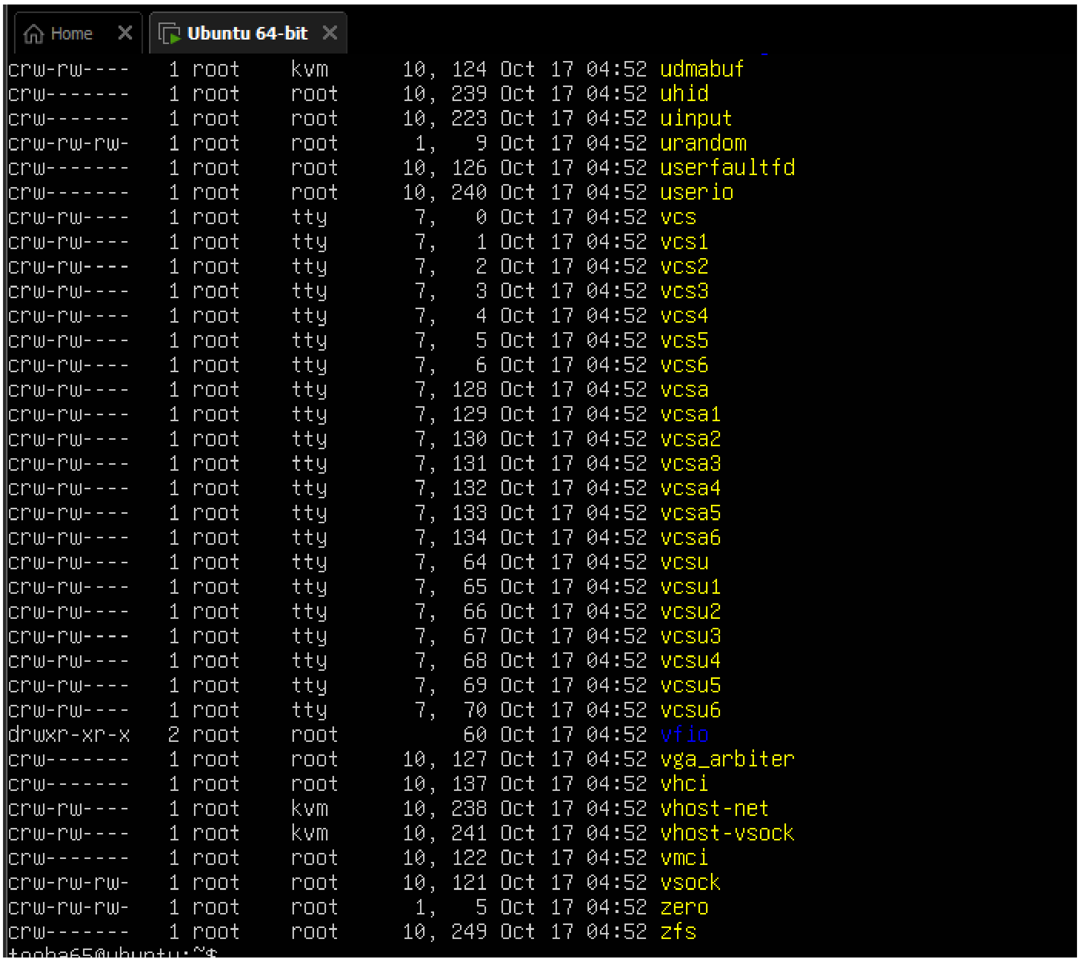
- Save screenshot as ls_etc.png



```
-rw-r--r--   1 root root         0 Aug  5 16:54 subuid-
-rw-r--r--   1 root root      4343 Jun 25 12:42 sudo.conf
-r--r-----   1 root root      1800 Jan 29  2024 sudoers
drwxr-xr-x   2 root root      4096 Aug  5 17:02 sudoers.d
-rw-r--r--   1 root root      9804 Jun 25 12:42 sudo_logsrvd.conf
drwxr-xr-x   2 root root      4096 Aug  5 17:14 supercat
-rw-r--r--   1 root root      2209 Mar 24  2024 sysctl.conf
drwxr-xr-x   2 root root      4096 Aug  5 17:02 sysctl.d
drwxr-xr-x   2 root root      4096 Aug  5 17:14 sysstat
drwxr-xr-x   6 root root      4096 Aug  5 16:49 systemd
drwxr-xr-x   2 root root      4096 Aug  5 17:00 terminfo
drwxr-xr-x   2 root root      4096 Oct  2 03:57 thermald
-rw-r--r--   1 root root         8 Aug  5 17:02 timezone
drwxr-xr-x   2 root root      4096 Aug  5 17:14 tmpfiles.d
drwxr-xr-x   2 root root      4096 Aug  5 17:14 ubuntu-advantage
-rw-r--r--   1 root root      1260 Jan 27  2023 ucf.conf
drwxr-xr-x   4 root root      4096 Aug  5 17:02 udev
drwxr-xr-x   2 root root      4096 Oct  2 04:00 udisks2
drwxr-xr-x   3 root root      4096 Aug  5 17:14 ufw
-rw-r--r--   1 root root       208 Aug  5 16:54 .updated
drwxr-xr-x   3 root root      4096 Aug  5 17:02 update-manager
drwxr-xr-x   2 root root      4096 Aug  5 17:14 update-motd.d
drwxr-xr-x   2 root root      4096 Aug  5 17:14 update-notifier
drwxr-xr-x   2 root root      4096 Oct  2 03:58 UPower
-rw-r--r--   1 root root      1523 Aug  5 17:14 usb_modeswitch.conf
drwxr-xr-x   2 root root      4096 Aug  5 17:14 usb_modeswitch.d
lrwxrwxrwx   1 root root        16 Aug  5 17:02 vconsole.conf -> default/keyboard
drwxr-xr-x   2 root root      4096 Oct  2 04:00 vim
drwxr-xr-x   4 root root      4096 Oct  2 04:00 vmware-tools
lrwxrwxrwx   1 root root        23 Feb 26  2024 vtrgb -> /etc/alternatives/vtrgb
-rw-r--r--   1 root root      4942 Aug  5 17:14 wgetrc
drwxr-xr-x   4 root root      4096 Aug  5 17:02 X11
-rw-r--r--   1 root root       681 Apr  8  2024 xattr.conf
drwxr-xr-x   4 root root      4096 Aug  5 17:02 xdg
drwxr-xr-x   2 root root      4096 Aug  5 17:02 xml
-rw-r--r--   1 root root       460 Aug  5 17:14 zsh_command_not_found
```

ls -la /dev

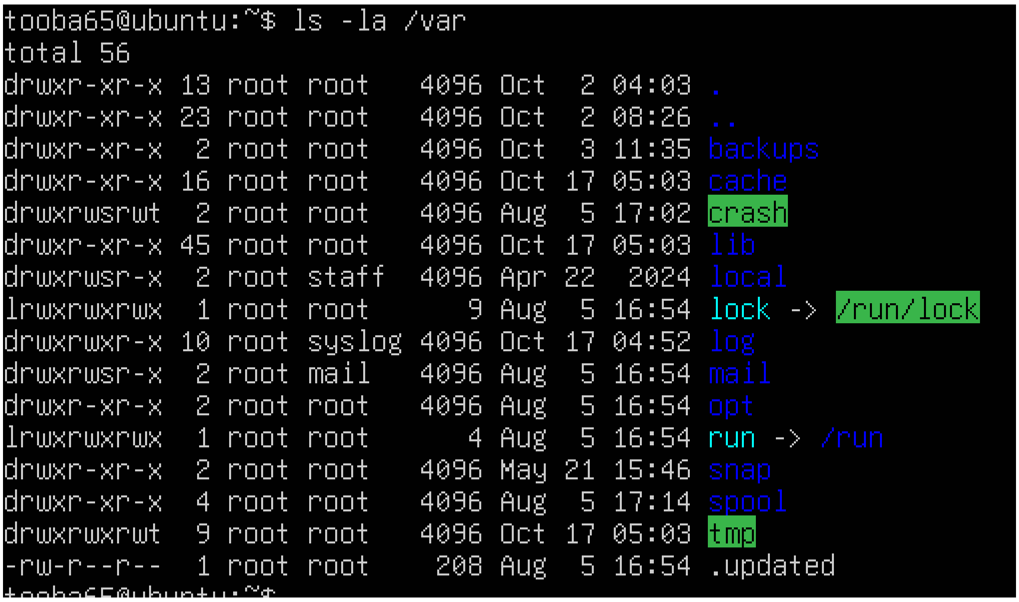
- Save screenshot as ls_dev.png



```
crw-rw----   1 root    kvm      10, 124 Oct 17 04:52 udmabuf
crw-------   1 root    root     10, 239 Oct 17 04:52 uhid
crw-------   1 root    root     10, 223 Oct 17 04:52 uinput
crw-rw-rw-   1 root    root      1,   9 Oct 17 04:52 urandom
crw-------   1 root    root     10, 126 Oct 17 04:52 userfaultfd
crw-------   1 root    root     10, 240 Oct 17 04:52 userio
crw-rw----   1 root    tty       7,   0 Oct 17 04:52 vcs
crw-rw----   1 root    tty       7,   1 Oct 17 04:52 vcs1
crw-rw----   1 root    tty       7,   2 Oct 17 04:52 vcs2
crw-rw----   1 root    tty       7,   3 Oct 17 04:52 vcs3
crw-rw----   1 root    tty       7,   4 Oct 17 04:52 vcs4
crw-rw----   1 root    tty       7,   5 Oct 17 04:52 vcs5
crw-rw----   1 root    tty       7,   6 Oct 17 04:52 vcs6
crw-rw----   1 root    tty       7, 128 Oct 17 04:52 vcsa
crw-rw----   1 root    tty       7, 129 Oct 17 04:52 vcsa1
crw-rw----   1 root    tty       7, 130 Oct 17 04:52 vcsa2
crw-rw----   1 root    tty       7, 131 Oct 17 04:52 vcsa3
crw-rw----   1 root    tty       7, 132 Oct 17 04:52 vcsa4
crw-rw----   1 root    tty       7, 133 Oct 17 04:52 vcsa5
crw-rw----   1 root    tty       7, 134 Oct 17 04:52 vcsa6
crw-rw----   1 root    tty       7,  64 Oct 17 04:52 vcsu
crw-rw----   1 root    tty       7,  65 Oct 17 04:52 vcsu1
crw-rw----   1 root    tty       7,  66 Oct 17 04:52 vcsu2
crw-rw----   1 root    tty       7,  67 Oct 17 04:52 vcsu3
crw-rw----   1 root    tty       7,  68 Oct 17 04:52 vcsu4
crw-rw----   1 root    tty       7,  69 Oct 17 04:52 vcsu5
crw-rw----   1 root    tty       7,  70 Oct 17 04:52 vcsu6
drwxr-xr-x   2 root    root          60 Oct 17 04:52 vfio
crw-------   1 root    root     10, 127 Oct 17 04:52 vga_arbiter
crw-------   1 root    root     10, 137 Oct 17 04:52 vhci
crw-rw----   1 root    kvm      10, 238 Oct 17 04:52 vhost-net
crw-rw----   1 root    kvm      10, 241 Oct 17 04:52 vhost-vsock
crw-------   1 root    root     10, 122 Oct 17 04:52 vmci
crw-rw-rw-   1 root    root     10, 121 Oct 17 04:52 vsock
crw-rw-rw-   1 root    root      1,   5 Oct 17 04:52 zero
crw-------   1 root    root     10, 249 Oct 17 04:52 zfs
tooba65@ubuntu:~$
```

ls -la /var

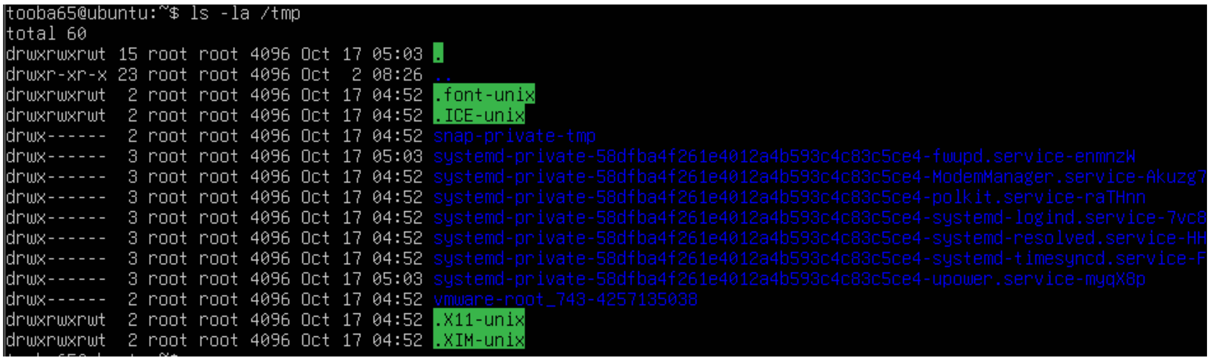
- Save screenshot as ls_var.png



```
tooba65@ubuntu:~$ ls -la /var
total 56
drwxr-xr-x 13 root root   4096 Oct  2 04:03 .
drwxr-xr-x 23 root root   4096 Oct  2 08:26 ..
drwxr-xr-x  2 root root   4096 Oct  3 11:35 backups
drwxr-xr-x 16 root root   4096 Oct 17 05:03 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Oct 17 05:03 lib
drwxrwsr-x  2 root staff  4096 Apr 22  2024 local
lrwxrwxrwx  1 root root      9 Aug  5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Oct 17 04:52 log
drwxrwsr-x  2 root mail   4096 Aug  5 16:54 mail
drwxr-xr-x  2 root root   4096 Aug  5 16:54 opt
lrwxrwxrwx  1 root root      4 Aug  5 16:54 run -> /run
drwxr-xr-x  2 root root   4096 May 21 15:46 snap
drwxr-xr-x  4 root root   4096 Aug  5 17:14 spool
drwxrwxrwt  9 root root   4096 Oct 17 05:03 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
tooba65@ubuntu:~$
```

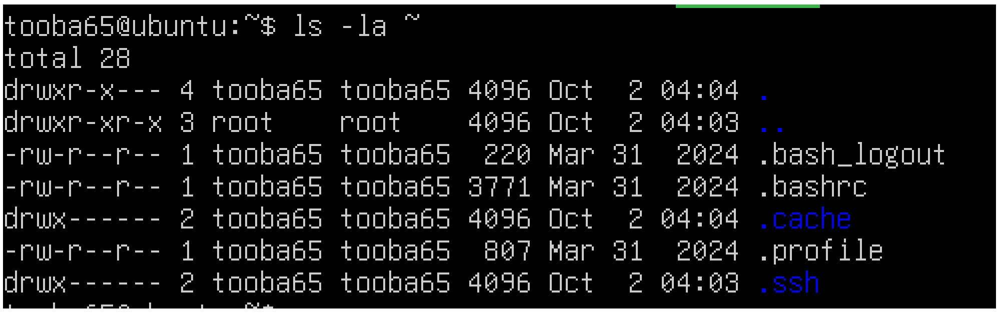
ls -la /tmp

- Save screenshot as ls_tmp.png



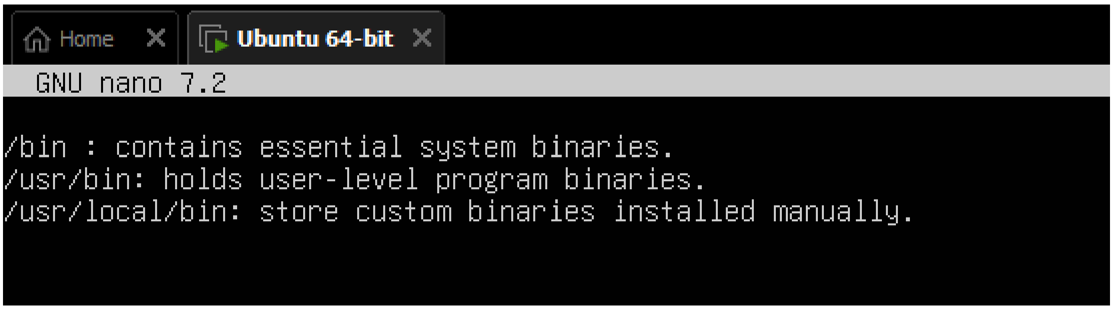
```
tooba65@ubuntu:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 17 05:03 .
drwxr-xr-x 23 root root 4096 Oct  2 08:26 ..
drwxrwxrwt  2 root root 4096 Oct 17 04:52 .font-unix
drwxrwxrwt  2 root root 4096 Oct 17 04:52 .ICE-unix
drwx------  2 root root 4096 Oct 17 04:52 snap-private-tmp
drwx------  3 root root 4096 Oct 17 05:03 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-fwupd.service-enmnzW
drwx------  3 root root 4096 Oct 17 04:52 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-ModemManager.service-Akuzg7
drwx------  3 root root 4096 Oct 17 04:52 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-polkit.service-raTHnn
drwx------  3 root root 4096 Oct 17 04:52 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-systemd-logind.service-7vc8
drwx------  3 root root 4096 Oct 17 04:52 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-systemd-resolved.service-HH
drwx------  3 root root 4096 Oct 17 04:52 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-systemd-timesyncd.service-F
drwx------  3 root root 4096 Oct 17 05:03 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-upower.service-myqX8p
drwx------  2 root root 4096 Oct 17 04:52 vmware-root_743-4257135038
drwxrwxrwt  2 root root 4096 Oct 17 04:52 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 17 04:52 .XIM-unix
```

Step 4: List your home directory and show hidden (dot) files
Screenshot: home_ls.png



```
tooba65@ubuntu:~$ ls -la ~
total 28
drwxr-x--- 4 tooba65 tooba65 4096 Oct  2 04:04 .
drwxr-xr-x 3 root    root    4096 Oct  2 04:03 ..
-rw-r--r-- 1 tooba65 tooba65  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 tooba65 tooba65 3771 Mar 31  2024 .bashrc
drwx------ 2 tooba65 tooba65 4096 Oct  2 04:04 .cache
-rw-r--r-- 1 tooba65 tooba65  807 Mar 31  2024 .profile
drwx------ 2 tooba65 tooba65 4096 Oct  2 04:03 .ssh
```

Step 5: Write a short paragraph (3–5 sentences) explaining the difference between /bin, /usr/bin, and /usr/local/bin.
Open a text editor inside the terminal to write and save your explanation.
Screenshot: answers_md.png

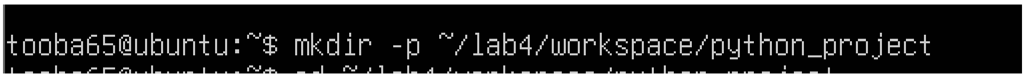


```
 GNU nano 7.2

/bin : contains essential system binaries.
/usr/bin: holds user-level program binaries.
/usr/local/bin: store custom binaries installed manually.
```

Task 4 – Essential CLI Tasks — Navigation and File Operations

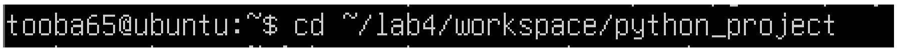
Steps

Step 1:
Create a workspace directory.
Save screenshot as: **mkdir_workspace.png**



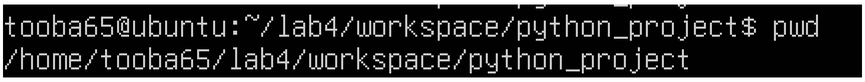
```
tooba65@ubuntu:~$ mkdir -p ~/lab4/workspace/python_project
```

Step 2:
Navigate to the newly created directory.
Save screenshot as: **cd_workspace.png**



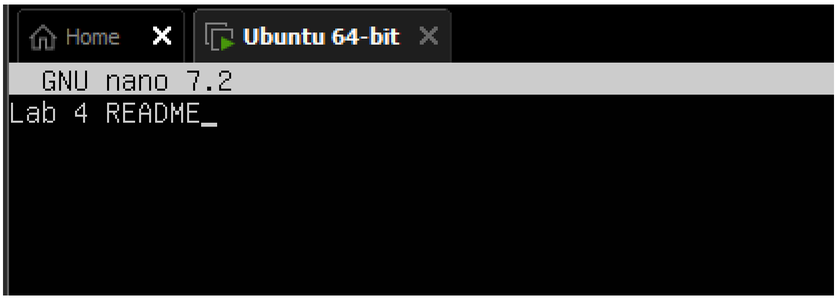
```
tooba65@ubuntu:~$ cd ~/lab4/workspace/python_project
```

Step 3:
Display your current directory path.
Save screenshot as: **pwd_workspace.png**



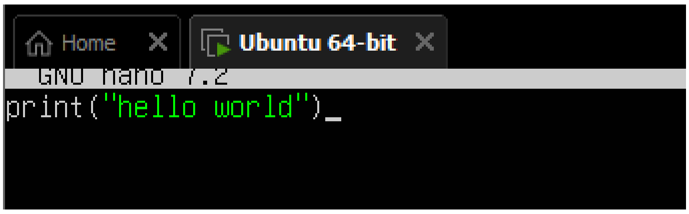
```
tooba65@ubuntu:~/lab4/workspace/python_project$ pwd
/home/tooba65/lab4/workspace/python_project
```

Step 4:
Create a new file using nano editor named README.md and type:
Lab 4 README
Save screenshot as: **nano_readme.png**



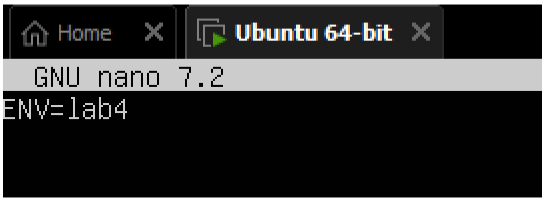
```
  GNU nano 7.2
Lab 4 README_
```

Step 5:
Create another file using nano editor named main.py and type:
print("hello lab4")
Save screenshot as: **nano_main.png**



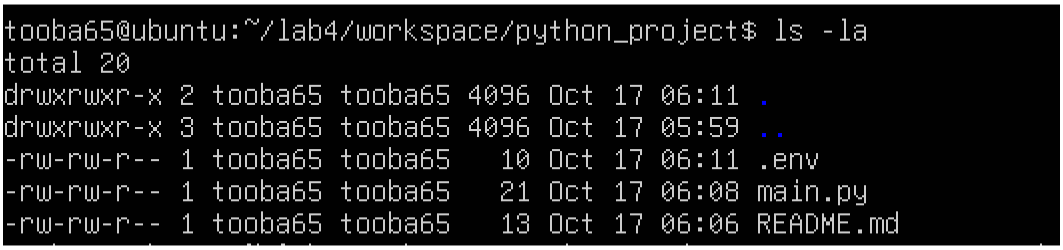
```
  GNU nano 7.2
print("hello world")_
```

Step 6:
Create an environment file named .env and type:
ENV=lab4
Save screenshot as: **nano_env.png**



```
  GNU nano 7.2
ENV=lab4
```

Step 7:
List all files (including hidden ones) in the current directory.
Save screenshot as: **workspace_ls.png**

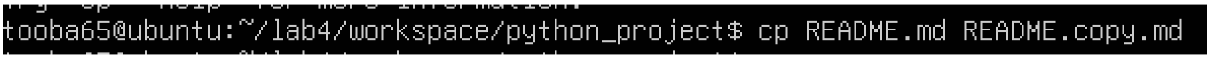


```
tooba65@ubuntu:~/lab4/workspace/python_project$ ls -la
total 20
drwxrwxr-x 2 tooba65 tooba65 4096 Oct 17 06:11 .
drwxrwxr-x 3 tooba65 tooba65 4096 Oct 17 05:59 ..
-rw-rw-r-- 1 tooba65 tooba65   10 Oct 17 06:11 .env
-rw-rw-r-- 1 tooba65 tooba65   21 Oct 17 06:08 main.py
-rw-rw-r-- 1 tooba65 tooba65   13 Oct 17 06:06 README.md
```

Step 8:

Copy the README file to a new file named README.copy.md.

Save screenshot as: **cp_readme.png**

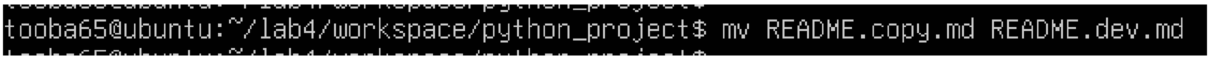


```
tooba65@ubuntu:~/lab4/workspace/python_project$ cp README.md README.copy.md
```

Step 9:

Rename (move) the copied file to README.dev.md.

Save screenshot as: **mv_readme.png**

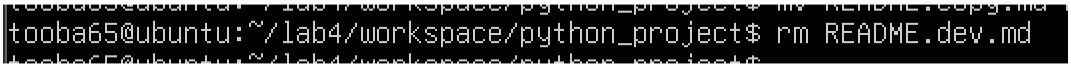


```
tooba65@ubuntu:~/lab4/workspace/python_project$ mv README.copy.md README.dev.md
```

Step 10:

Remove the README.dev.md file.

Save screenshot as: **rm_readme.png**



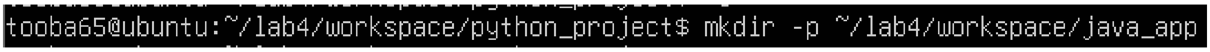
```
tooba65@ubuntu:~/lab4/workspace/python_project$ rm README.dev.md
```

Step 11:

Create a new directory for Java work:

java_app

Save screenshot as: **mkdir_java_app.png**

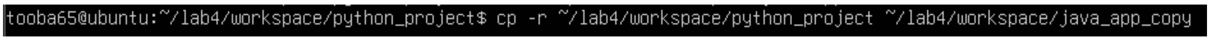


```
tooba65@ubuntu:~/lab4/workspace/python_project$ mkdir -p ~/lab4/workspace/java_app
```

Step 12:

Copy the entire python_project folder into a new folder named java_app_copy.

Save screenshot as: **cp_recursive.png**

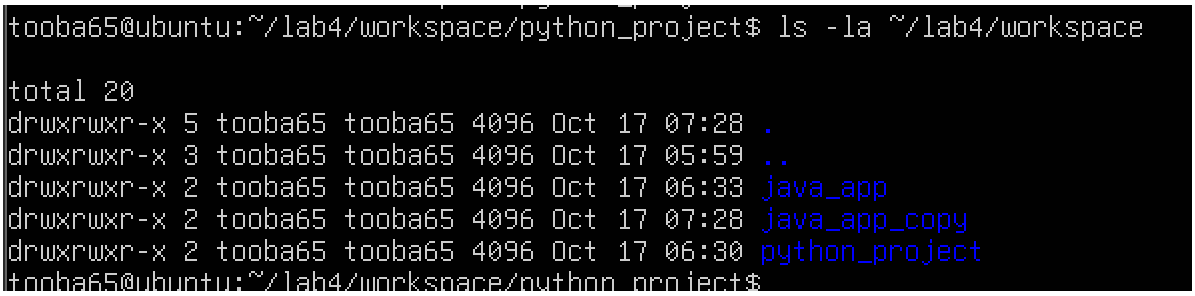


```
tooba65@ubuntu:~/lab4/workspace/python_project$ cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
```

Step 13:

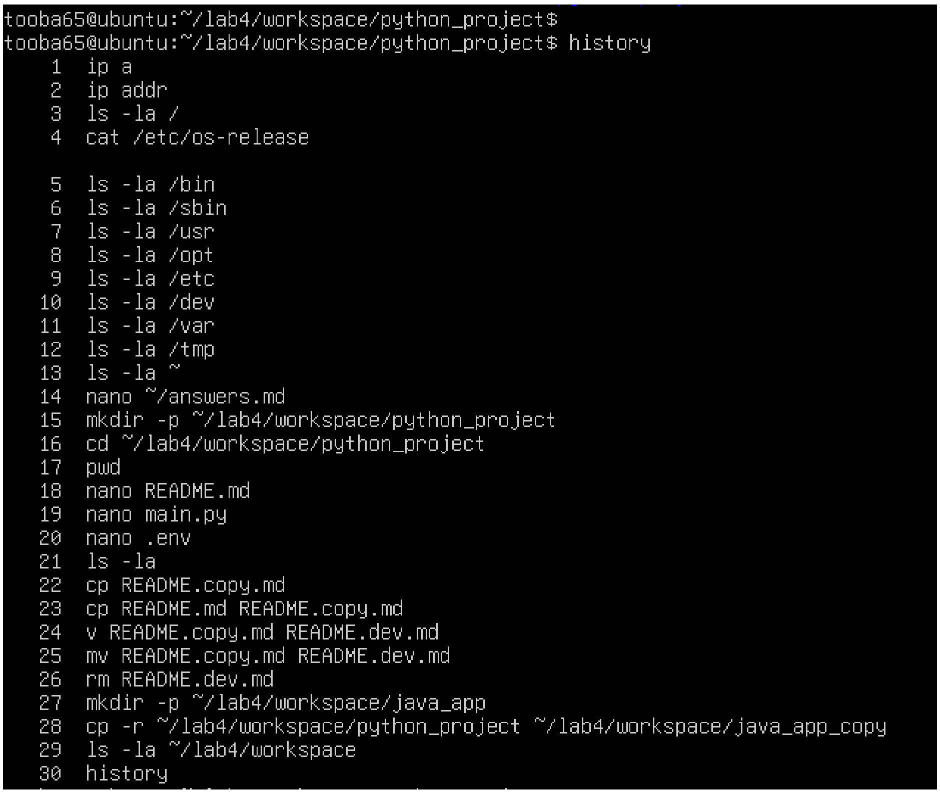
List all directories inside workspace to verify the copy.

Save screenshot as: **copy_verify.png**



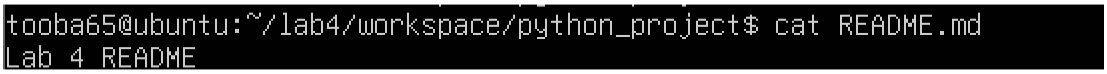
```
tooba65@ubuntu:~/lab4/workspace/python_project$ ls -la ~/lab4/workspace

total 20
drwxrwxr-x 5 tooba65 tooba65 4096 Oct 17 07:28 .
drwxrwxr-x 3 tooba65 tooba65 4096 Oct 17 05:59 ..
drwxrwxr-x 2 tooba65 tooba65 4096 Oct 17 06:33 java_app
drwxrwxr-x 2 tooba65 tooba65 4096 Oct 17 07:28 java_app_copy
drwxrwxr-x 2 tooba65 tooba65 4096 Oct 17 06:30 python_project
tooba65@ubuntu:~/lab4/workspace/python_project$
```

Step 14:
Show recent command history.
Save screenshot as: **history.png**



```
tooba65@ubuntu:~/lab4/workspace/python_project$
tooba65@ubuntu:~/lab4/workspace/python_project$ history
    1  ip a
    2  ip addr
    3  ls -la /
    4  cat /etc/os-release

    5  ls -la /bin
    6  ls -la /sbin
    7  ls -la /usr
    8  ls -la /opt
    9  ls -la /etc
   10  ls -la /dev
   11  ls -la /var
   12  ls -la /tmp
   13  ls -la ~
   14  nano ~/answers.md
   15  mkdir -p ~/lab4/workspace/python_project
   16  cd ~/lab4/workspace/python_project
   17  pwd
   18  nano README.md
   19  nano main.py
   20  nano .env
   21  ls -la
   22  cp README.copy.md
   23  cp README.md README.copy.md
   24  v README.copy.md README.dev.md
   25  mv README.copy.md README.dev.md
   26  rm README.dev.md
   27  mkdir -p ~/lab4/workspace/java_app
   28  cp -r ~/lab4/workspace/python_project ~/lab4/workspace/java_app_copy
   29  ls -la ~/lab4/workspace
   30  history
```

Step 15:
Demonstrate tab completion (start typing a filename and press **Tab** to auto-complete).
Save screenshot as: **tab_completion.png**



```
tooba65@ubuntu:~/lab4/workspace/python_project$ cat README.md
Lab 4 README
```

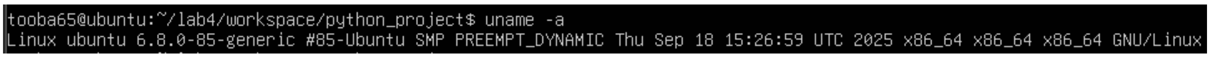
Task 5 – System info, resources & processes

Collect system information and observe processes. Use screenshots only.

Steps (inside VM terminal)

Step 1: Kernel and OS

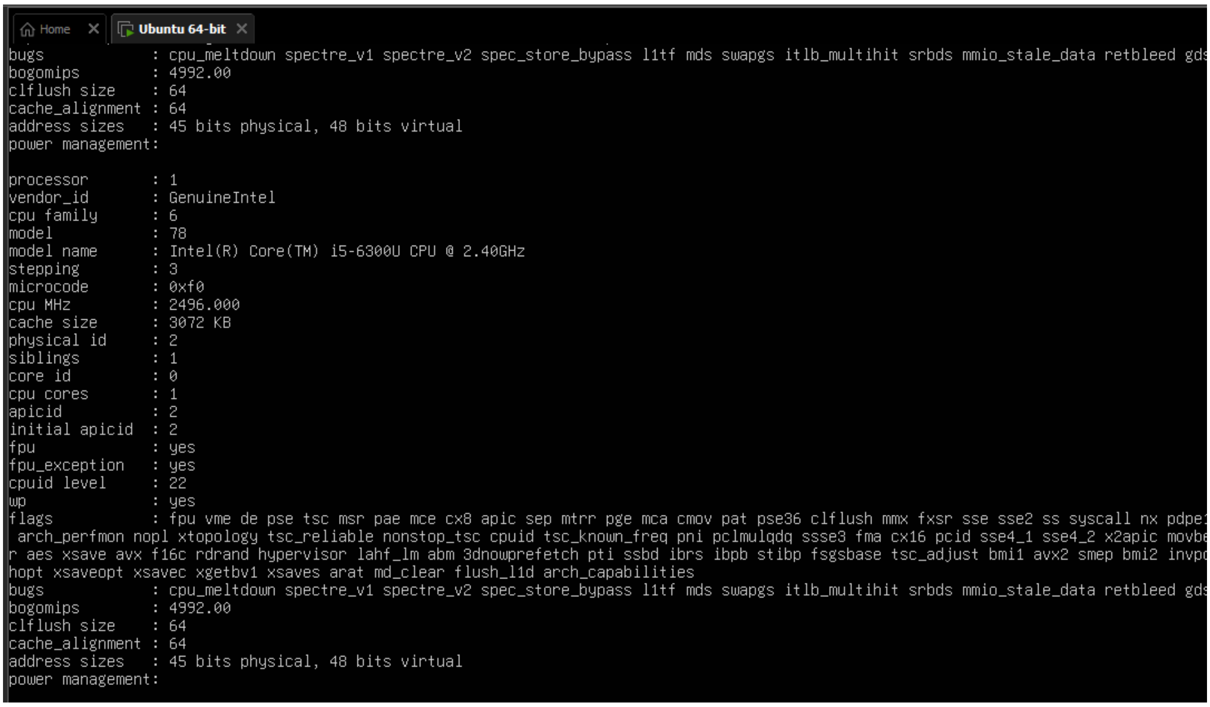
Save screenshot as uname.png.



```
tooba65@ubuntu:~/lab4/workspace/python_project$ uname -a
Linux ubuntu 6.8.0-85-generic #85-Ubuntu SMP PREEMPT_DYNAMIC Thu Sep 18 15:26:59 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
```

Step 2: CPU (ensure model name visible):

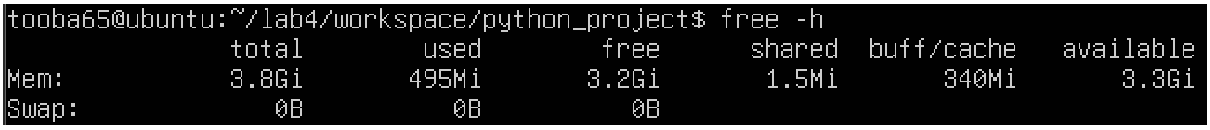
Save screenshot as cpuinfo.png.



```
bugs            : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbds mmio_stale_data retbleed gds
bogomips        : 4992.00
clflush size    : 64
cache_alignment : 64
address sizes   : 45 bits physical, 48 bits virtual
power management:

processor       : 1
vendor_id       : GenuineIntel
cpu family      : 6
model           : 78
model name      : Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
stepping        : 3
microcode       : 0xf0
cpu MHz         : 2496.000
cache size      : 3072 KB
physical id     : 2
siblings        : 1
core id         : 0
cpu cores       : 1
apicid          : 2
initial apicid  : 2
fpu             : yes
fpu_exception   : yes
cpuid level     : 22
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1
 arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe
r aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpc
hopt xsaveopt xsavec xgetbv1 xsaves arat md_clear flush_l1d arch_capabilities
bugs            : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbds mmio_stale_data retbleed gds
bogomips        : 4992.00
clflush size    : 64
cache_alignment : 64
address sizes   : 45 bits physical, 48 bits virtual
power management:
```

Step 3: Memory:

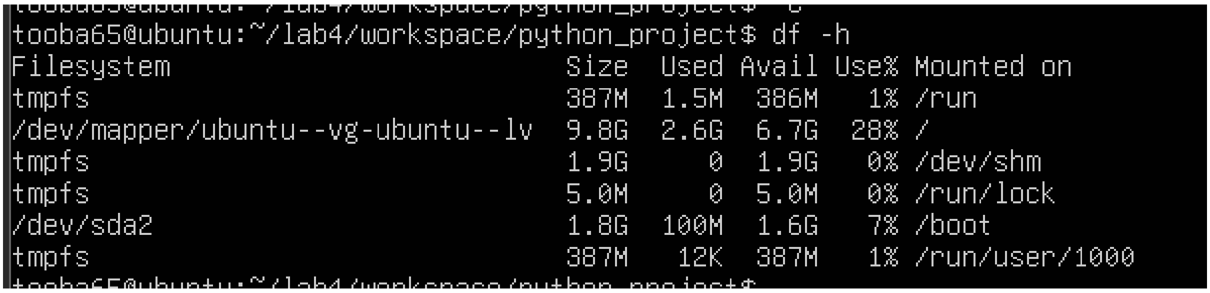
Save screenshot as meminfo.png.



```
tooba65@ubuntu:~/lab4/workspace/python_project$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       495Mi       3.2Gi       1.5Mi       340Mi       3.3Gi
Swap:             0B          0B          0B
```

Step 4: Disk:

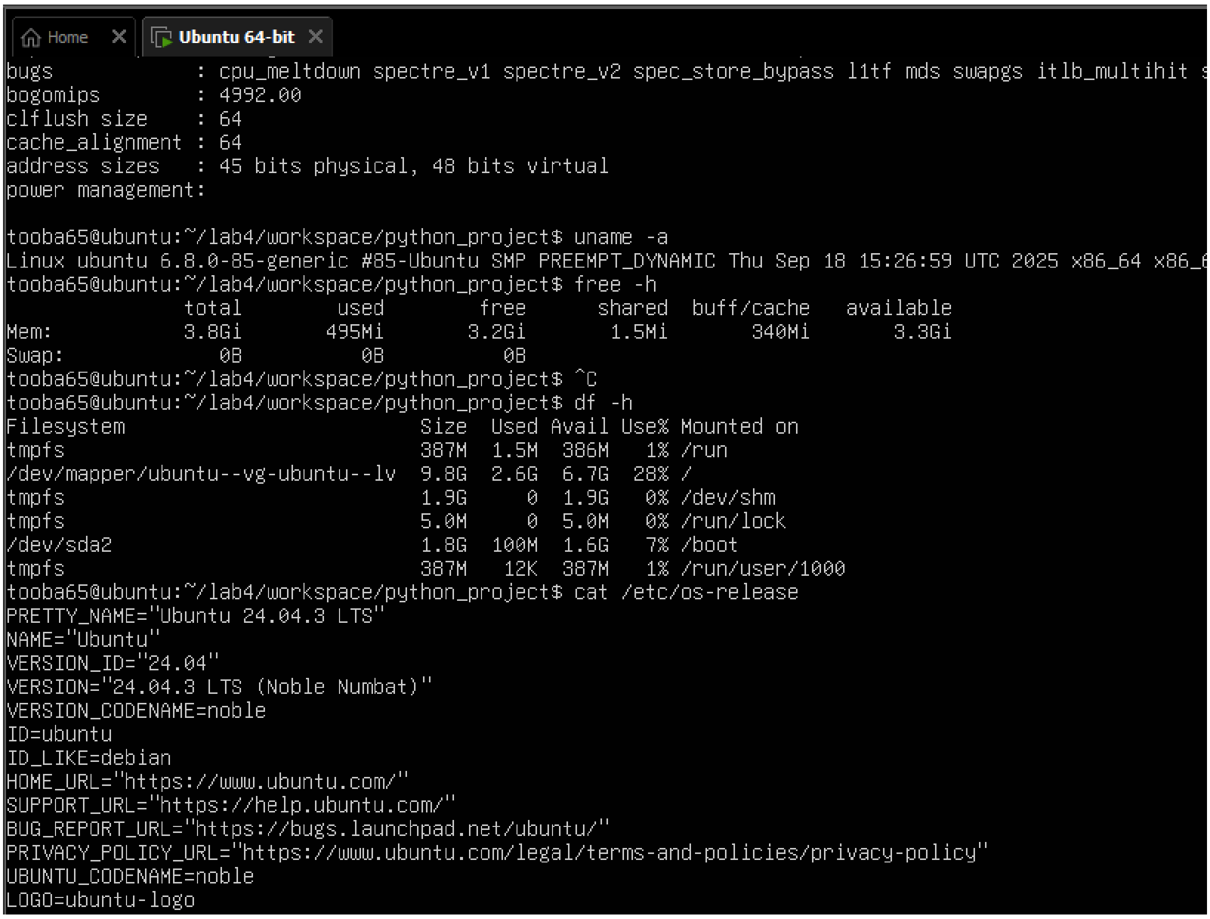
Save screenshot as diskinfo.png.



```
tooba65@ubuntu:~/lab4/workspace/python_project$ c
tooba65@ubuntu:~/lab4/workspace/python_project$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              387M  1.5M  386M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  9.8G  2.6G  6.7G  28% /
tmpfs                              1.9G     0  1.9G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          1.8G  100M  1.6G   7% /boot
tmpfs                              387M   12K  387M   1% /run/user/1000
tooba65@ubuntu:~/lab4/workspace/python_project$
```

Step 5: Os Release:

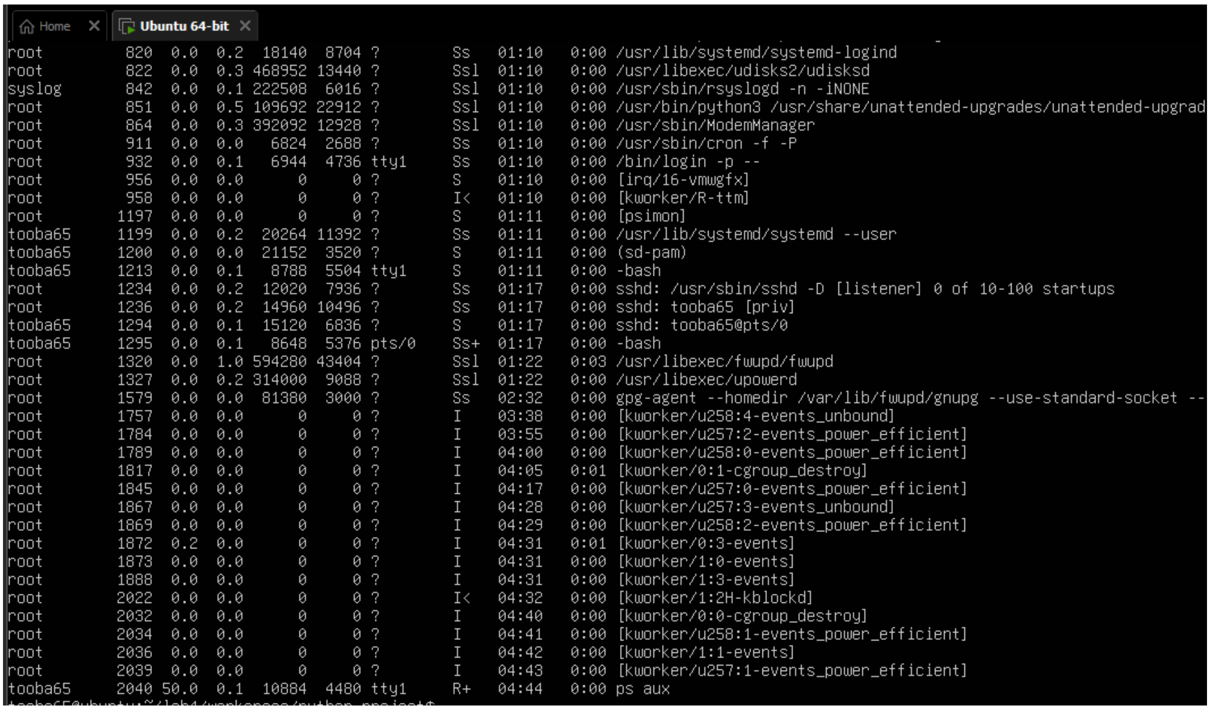
Save screenshot as os-release.png.



```
bugs            : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit s
bogomips        : 4992.00
clflush size    : 64
cache_alignment : 64
address sizes   : 45 bits physical, 48 bits virtual
power management:

tooba65@ubuntu:~/lab4/workspace/python_project$ uname -a
Linux ubuntu 6.8.0-85-generic #85-Ubuntu SMP PREEMPT_DYNAMIC Thu Sep 18 15:26:59 UTC 2025 x86_64 x86_6
tooba65@ubuntu:~/lab4/workspace/python_project$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       495Mi       3.2Gi       1.5Mi       340Mi       3.3Gi
Swap:             0B          0B          0B
tooba65@ubuntu:~/lab4/workspace/python_project$ ^C
tooba65@ubuntu:~/lab4/workspace/python_project$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              387M  1.5M  386M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  9.8G  2.6G  6.7G  28% /
tmpfs                              1.9G     0  1.9G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          1.8G  100M  1.6G   7% /boot
tmpfs                              387M   12K  387M   1% /run/user/1000
tooba65@ubuntu:~/lab4/workspace/python_project$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
```

Step 6: Processes (show top lines of ps output):

- Save screenshot as processes.png



```
root         820  0.0  0.2  18140  8704 ?        Ss   01:10   0:00 /usr/lib/systemd/systemd-logind
root         822  0.0  0.3 468952 13440 ?        Ssl  01:10   0:00 /usr/libexec/udisks2/udisksd
syslog       842  0.0  0.1 222508  6016 ?        Ssl  01:10   0:00 /usr/sbin/rsyslogd -n -iNONE
root         851  0.0  0.5 109692 22912 ?        Ssl  01:10   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrad
root         864  0.0  0.3 392092 12928 ?        Ssl  01:10   0:00 /usr/sbin/ModemManager
root         911  0.0  0.0   6824  2688 ?        Ss   01:10   0:00 /usr/sbin/cron -f -P
root         932  0.0  0.1   6944  4736 tty1     Ss   01:10   0:00 /bin/login -p --
root         956  0.0  0.0      0     0 ?        S    01:10   0:00 [irq/16-vmwgfx]
root         958  0.0  0.0      0     0 ?        I<   01:10   0:00 [kworker/R-ttm]
root        1197  0.0  0.0      0     0 ?        S    01:11   0:00 [psimon]
tooba65     1199  0.0  0.2  20264 11392 ?        Ss   01:11   0:00 /usr/lib/systemd/systemd --user
tooba65     1200  0.0  0.0  21152  3520 ?        S    01:11   0:00 (sd-pam)
tooba65     1213  0.0  0.1   8788  5504 tty1     S    01:11   0:00 -bash
root        1234  0.0  0.2  12020  7936 ?        Ss   01:17   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        1236  0.0  0.2  14960 10496 ?        Ss   01:17   0:00 sshd: tooba65 [priv]
tooba65     1294  0.0  0.1  15120  6836 ?        S    01:17   0:00 sshd: tooba65@pts/0
tooba65     1295  0.0  0.1   8648  5376 pts/0    Ss+  01:17   0:00 -bash
root        1320  0.0  1.0 594280 43404 ?        Ssl  01:22   0:03 /usr/libexec/fwupd/fwupd
root        1327  0.0  0.2 314000  9088 ?        Ssl  01:22   0:00 /usr/libexec/upowerd
root        1579  0.0  0.0  81380  3000 ?        Ss   02:32   0:00 gpg-agent --homedir /var/lib/fwupd/gnupg --use-standard-socket --
root        1757  0.0  0.0      0     0 ?        I    03:38   0:00 [kworker/u258:4-events_unbound]
root        1784  0.0  0.0      0     0 ?        I    03:55   0:00 [kworker/u257:2-events_power_efficient]
root        1789  0.0  0.0      0     0 ?        I    04:00   0:00 [kworker/u258:0-events_power_efficient]
root        1817  0.0  0.0      0     0 ?        I    04:05   0:01 [kworker/0:1-cgroup_destroy]
root        1845  0.0  0.0      0     0 ?        I    04:17   0:00 [kworker/u257:0-events_power_efficient]
root        1867  0.0  0.0      0     0 ?        I    04:28   0:00 [kworker/u257:3-events_unbound]
root        1869  0.0  0.0      0     0 ?        I    04:29   0:00 [kworker/u258:2-events_power_efficient]
root        1872  0.2  0.0      0     0 ?        I    04:31   0:01 [kworker/0:3-events]
root        1873  0.0  0.0      0     0 ?        I    04:31   0:00 [kworker/1:0-events]
root        1888  0.0  0.0      0     0 ?        I    04:31   0:00 [kworker/1:3-events]
root        2022  0.0  0.0      0     0 ?        I<   04:32   0:00 [kworker/1:2H-kblockd]
root        2032  0.0  0.0      0     0 ?        I    04:40   0:00 [kworker/0:0-cgroup_destroy]
root        2034  0.0  0.0      0     0 ?        I    04:41   0:00 [kworker/u258:1-events_power_efficient]
root        2036  0.0  0.0      0     0 ?        I    04:42   0:00 [kworker/1:1-events]
root        2039  0.0  0.0      0     0 ?        I    04:43   0:00 [kworker/u257:1-events_power_efficient]
tooba65     2040 50.0  0.1  10884  4480 tty1     R+   04:44   0:00 ps aux
```

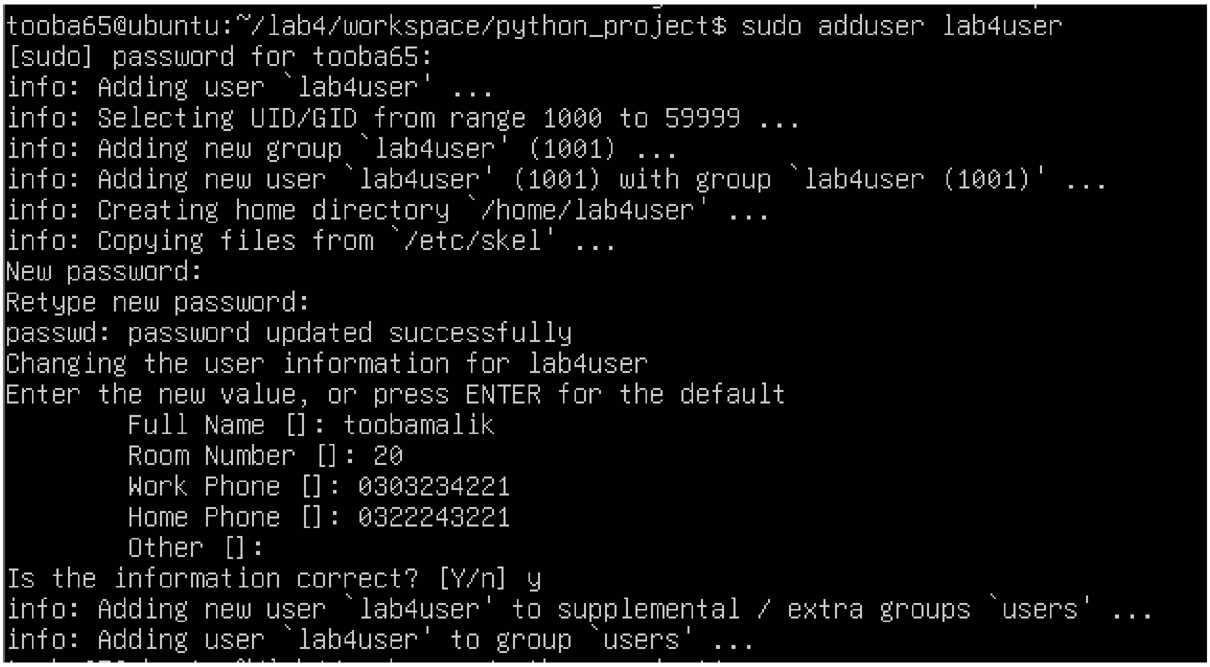
Task 6 – Users and account verification (no sudo group change)

Create a non-root user and verify the account exists. This task does NOT add the created user to the sudo group.

Steps (inside VM terminal)

Step 1: Create a new user named lab4user:

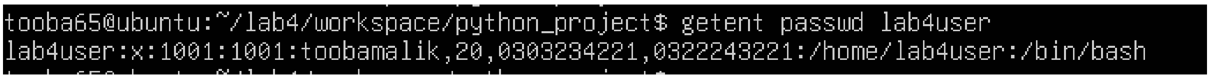
- During prompts, capture the terminal and save screenshot as adduser_lab4user.png.



```
tooba65@ubuntu:~/lab4/workspace/python_project$ sudo adduser lab4user
[sudo] password for tooba65:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1001) ...
info: Adding new user `lab4user' (1001) with group `lab4user (1001)' ...
info: Creating home directory `/home/lab4user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lab4user
Enter the new value, or press ENTER for the default
        Full Name []: toobamalik
        Room Number []: 20
        Work Phone []: 0303234221
        Home Phone []: 0322243221
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
```

Step 2: Verify the user entry:

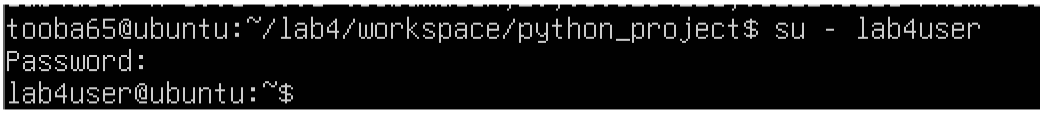
- Save screenshot as lab4user_passwd.png.



```
tooba65@ubuntu:~/lab4/workspace/python_project$ getent passwd lab4user
lab4user:x:1001:1001:toobamalik,20,0303234221,0322243221:/home/lab4user:/bin/bash
```

Step 3: Switch to the new user to verify login:

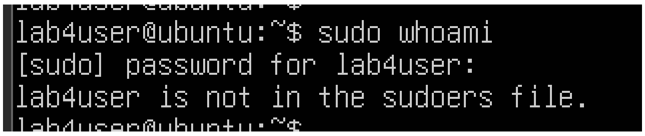
- Save screenshot as su_lab4user.png.



```
tooba65@ubuntu:~/lab4/workspace/python_project$ su - lab4user
Password:
lab4user@ubuntu:~$
```

Step 4: From the new user you may attempt a sudo command to show that sudo is not available for this account (expected failure), e.g.:

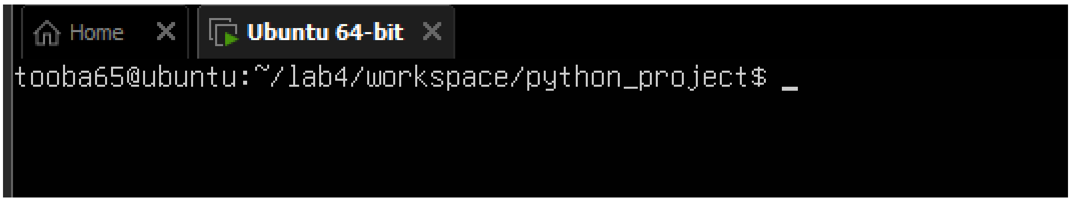
- Save screenshot as sudo_whoami.png.



```
lab4user@ubuntu:~$ sudo whoami
[sudo] password for lab4user:
lab4user is not in the sudoers file.
lab4user@ubuntu:~$
```

Step 5: Return to the original user:

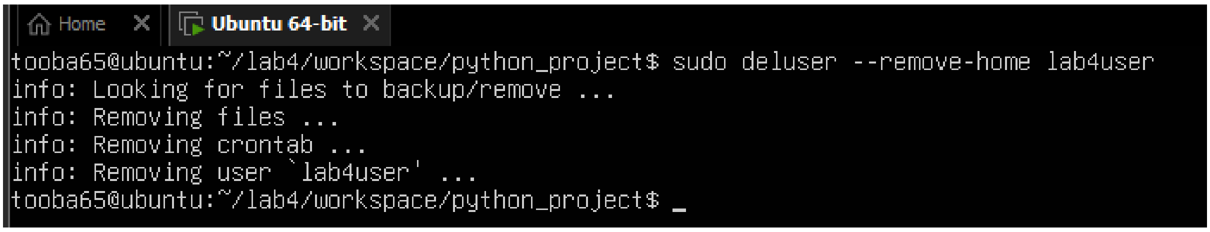
- Save screenshot as exit_back.png.
- When I exit it moves to the original user.



```
tooba65@ubuntu:~/lab4/workspace/python_project$ _
```

Step 6: (Optional) Remove the test user when finished:

- If run, save screenshot as deluser.png.



```
tooba65@ubuntu:~/lab4/workspace/python_project$ sudo deluser --remove-home lab4user
info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
tooba65@ubuntu:~/lab4/workspace/python_project$ _
```

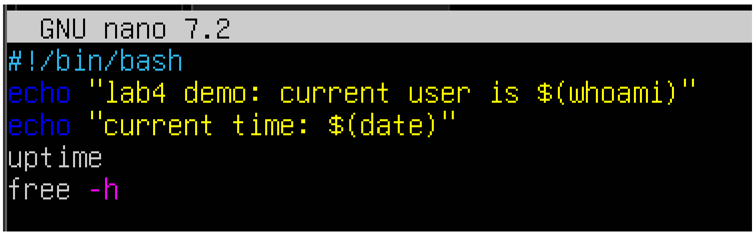
Bonus Task 7 – Create a small demo script using an editor and run it

This task is optional — complete it for extra practice or extra credit. It is not required for passing the core lab tasks.

Steps (inside VM)

Step 1: Open an editor to create the script:

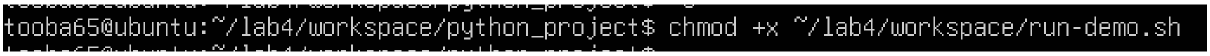
- Type the following lines into the editor (manually or paste), save and exit:
- Save screenshot of the editor after saving the file as nano_run_demo.png.



```
  GNU nano 7.2
#!/bin/bash
echo "lab4 demo: current user is $(whoami)"
echo "current time: $(date)"
uptime
free -h
```

Step 2: Make the script executable:

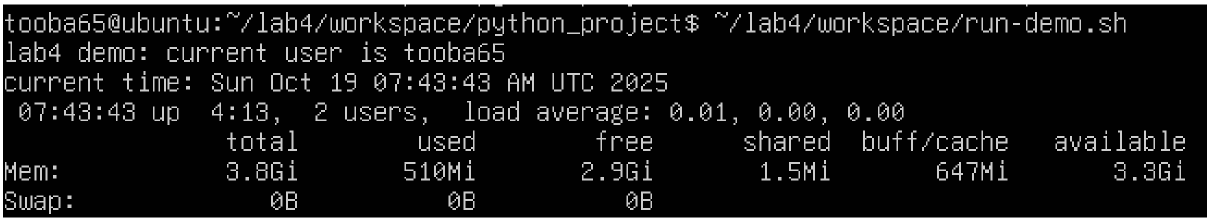
- Save screenshot as chmod_run_demo.png.



```
tooba65@ubuntu:~/lab4/workspace/python_project$ chmod +x ~/lab4/workspace/run-demo.sh
```

Step 3: Run the script as your regular user:

- Save screenshot of the script output as run_demo_output.png.



```
tooba65@ubuntu:~/lab4/workspace/python_project$ ~/lab4/workspace/run-demo.sh
lab4 demo: current user is tooba65
current time: Sun Oct 19 07:43:43 AM UTC 2025
 07:43:43 up  4:13,  2 users,  load average: 0.01, 0.00, 0.00
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       510Mi       2.9Gi       1.5Mi       647Mi       3.3Gi
Swap:             0B          0B          0B
```

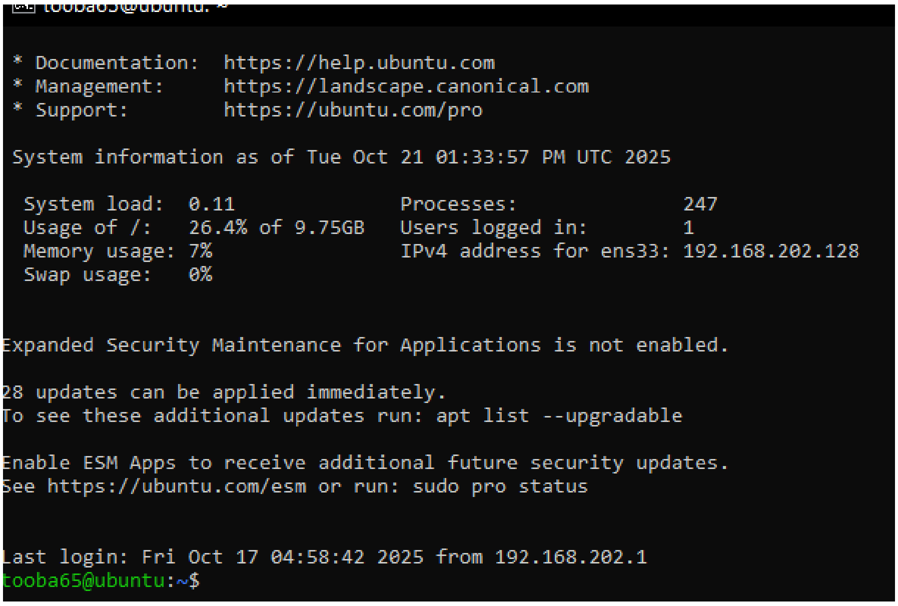
Exam Evaluation Questions

1. Remote Access Verification (Cyber Login Check)

Scenario:
You are part of a SOC (Security Operations Center) investigating unauthorized access to a Linux server hosted on VMware. Prove you can securely connect and verify your identity.

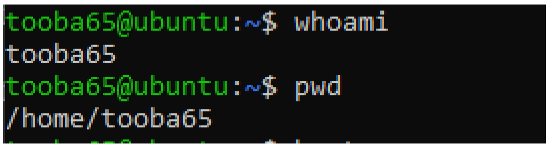
Steps:

1. Connect to the Ubuntu VM remotely from your host terminal.
   - Screenshot as Q1_remote_connection.png



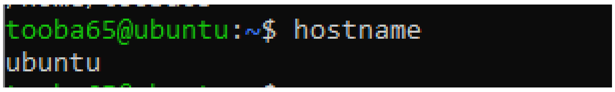
```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Oct 21 01:33:57 PM UTC 2025

  System load:  0.11               Processes:             247
  Usage of /:   26.4% of 9.75GB    Users logged in:       1
  Memory usage: 7%                 IPv4 address for ens33: 192.168.202.128
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

28 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Fri Oct 17 04:58:42 2025 from 192.168.202.1
tooba65@ubuntu:~$
```

2. Verify your current user and home directory path.
   - Screenshot as Q1_user_verification.png



```
tooba65@ubuntu:~$ whoami
tooba65
tooba65@ubuntu:~$ pwd
/home/tooba65
```

3. Confirm you are connected to the correct host machine.
   - Screenshot as Q1_host_confirmation.png



```
tooba65@ubuntu:~$ hostname
ubuntu
```

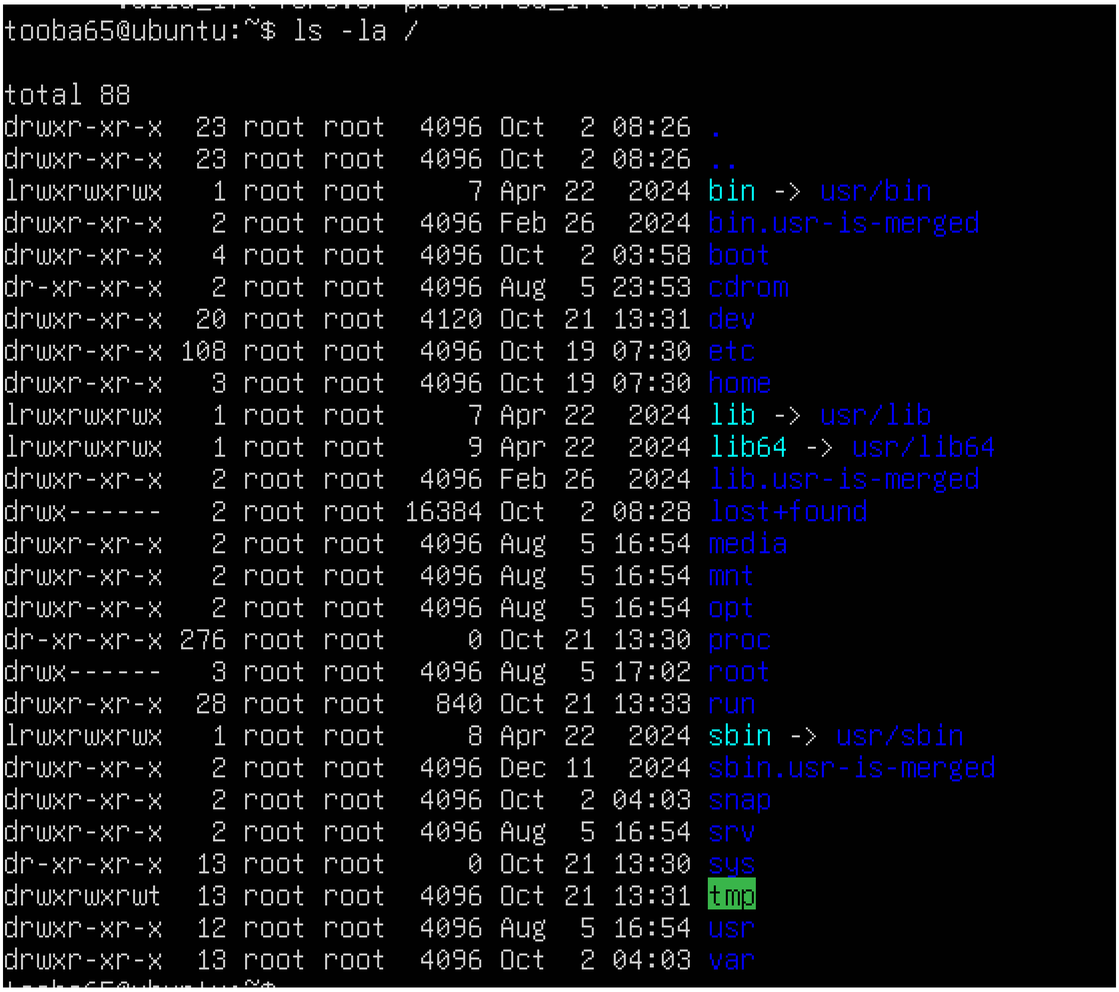
---

2. Filesystem Inspection for Forensic Evidence

Scenario:
The incident response team suspects malicious files in system directories. You must explore the filesystem to locate and document the system’s structure.

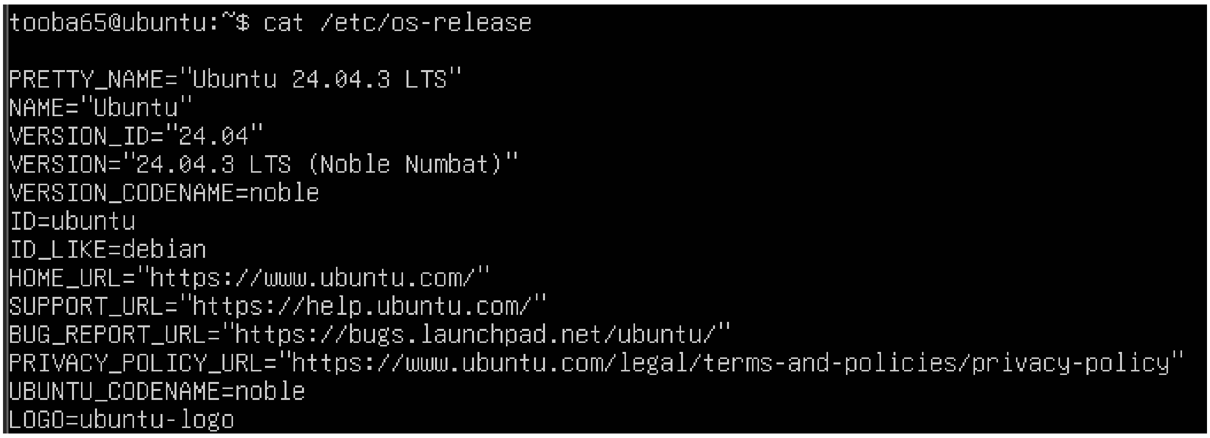
Steps:

1. Display the contents of the root directory.
   - Screenshot as Q2_root_listing.png



```
    valid_lft forever preferred_lft forever
tooba65@ubuntu:~$ ls -la /

total 88
drwxr-xr-x  23 root root  4096 Oct  2 08:26 .
drwxr-xr-x  23 root root  4096 Oct  2 08:26 ..
lrwxrwxrwx   1 root root     7 Apr 22  2024 bin -> usr/bin
drwxr-xr-x   2 root root  4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x   4 root root  4096 Oct  2 03:58 boot
dr-xr-xr-x   2 root root  4096 Aug  5 23:53 cdrom
drwxr-xr-x  20 root root  4120 Oct 21 13:31 dev
drwxr-xr-x 108 root root  4096 Oct 19 07:30 etc
drwxr-xr-x   3 root root  4096 Oct 19 07:30 home
lrwxrwxrwx   1 root root     7 Apr 22  2024 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Apr 22  2024 lib64 -> usr/lib64
drwxr-xr-x   2 root root  4096 Feb 26  2024 lib.usr-is-merged
drwx------   2 root root 16384 Oct  2 08:28 lost+found
drwxr-xr-x   2 root root  4096 Aug  5 16:54 media
drwxr-xr-x   2 root root  4096 Aug  5 16:54 mnt
drwxr-xr-x   2 root root  4096 Aug  5 16:54 opt
dr-xr-xr-x 276 root root     0 Oct 21 13:30 proc
drwx------   3 root root  4096 Aug  5 17:02 root
drwxr-xr-x  28 root root   840 Oct 21 13:33 run
lrwxrwxrwx   1 root root     8 Apr 22  2024 sbin -> usr/sbin
drwxr-xr-x   2 root root  4096 Dec 11  2024 sbin.usr-is-merged
drwxr-xr-x   2 root root  4096 Oct  2 04:03 snap
drwxr-xr-x   2 root root  4096 Aug  5 16:54 srv
dr-xr-xr-x  13 root root     0 Oct 21 13:30 sys
drwxrwxrwt  13 root root  4096 Oct 21 13:31 tmp
drwxr-xr-x  12 root root  4096 Aug  5 16:54 usr
drwxr-xr-x  13 root root  4096 Oct  2 04:03 var
tooba65@ubuntu:~$
```

2. Display the OS version and release information.
   - Screenshot as Q2_os_version.png

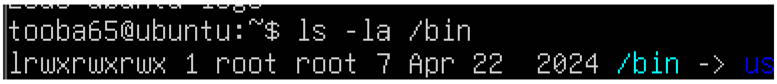


```
tooba65@ubuntu:~$ cat /etc/os-release

PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
```

3. Explore and record directory listings for /bin, /sbin, /usr, /opt, /etc, /dev, /var, and /tmp.

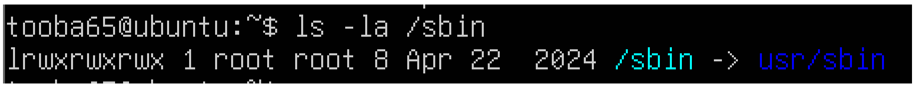
   - Screenshot as Q2_directory_evidence.png

ls -la /bin



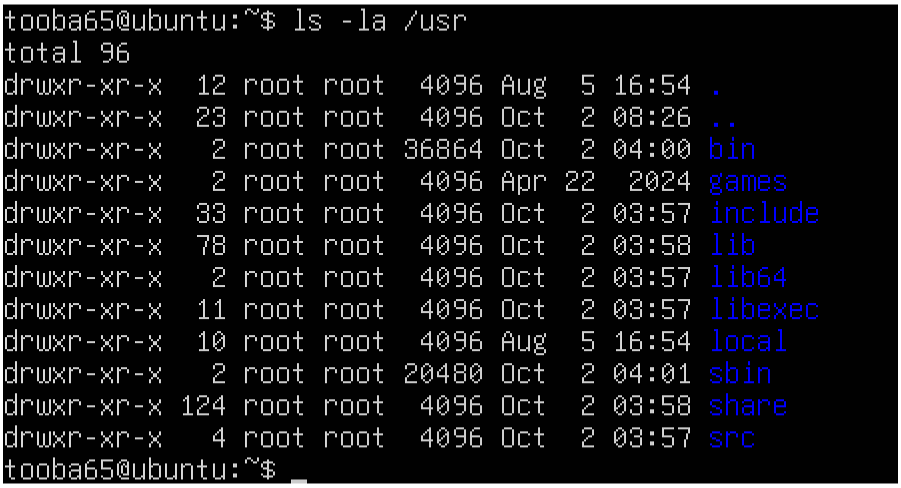
```
LOGO=ubuntu-logo
tooba65@ubuntu:~$ ls -la /bin
lrwxrwxrwx 1 root root 7 Apr 22  2024 /bin -> us
```

ls -la /sbin



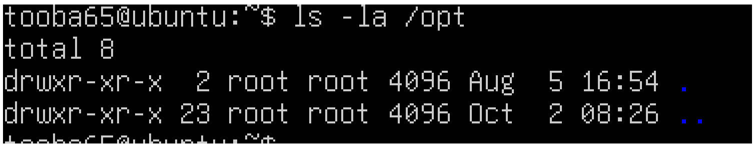
```
tooba65@ubuntu:~$ ls -la /sbin
lrwxrwxrwx 1 root root 8 Apr 22  2024 /sbin -> usr/sbin
```

ls -la /usr



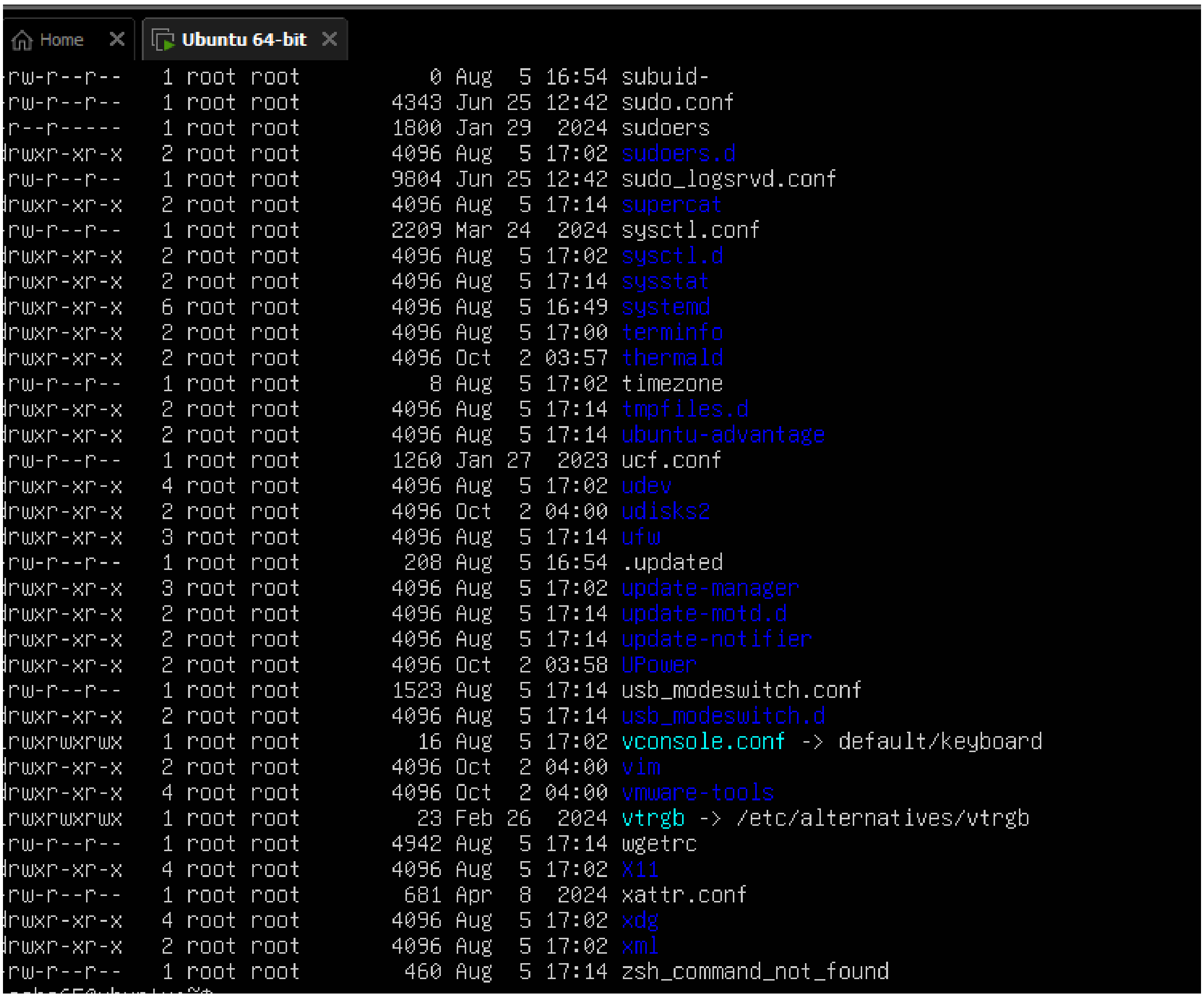
```
tooba65@ubuntu:~$ ls -la /usr
total 96
drwxr-xr-x  12 root root  4096 Aug  5 16:54 .
drwxr-xr-x  23 root root  4096 Oct  2 08:26 ..
drwxr-xr-x   2 root root 36864 Oct  2 04:00 bin
drwxr-xr-x   2 root root  4096 Apr 22  2024 games
drwxr-xr-x  33 root root  4096 Oct  2 03:57 include
drwxr-xr-x  78 root root  4096 Oct  2 03:58 lib
drwxr-xr-x   2 root root  4096 Oct  2 03:57 lib64
drwxr-xr-x  11 root root  4096 Oct  2 03:57 libexec
drwxr-xr-x  10 root root  4096 Aug  5 16:54 local
drwxr-xr-x   2 root root 20480 Oct  2 04:01 sbin
drwxr-xr-x 124 root root  4096 Oct  2 03:58 share
drwxr-xr-x   4 root root  4096 Oct  2 03:57 src
tooba65@ubuntu:~$ _
```

ls -la /opt



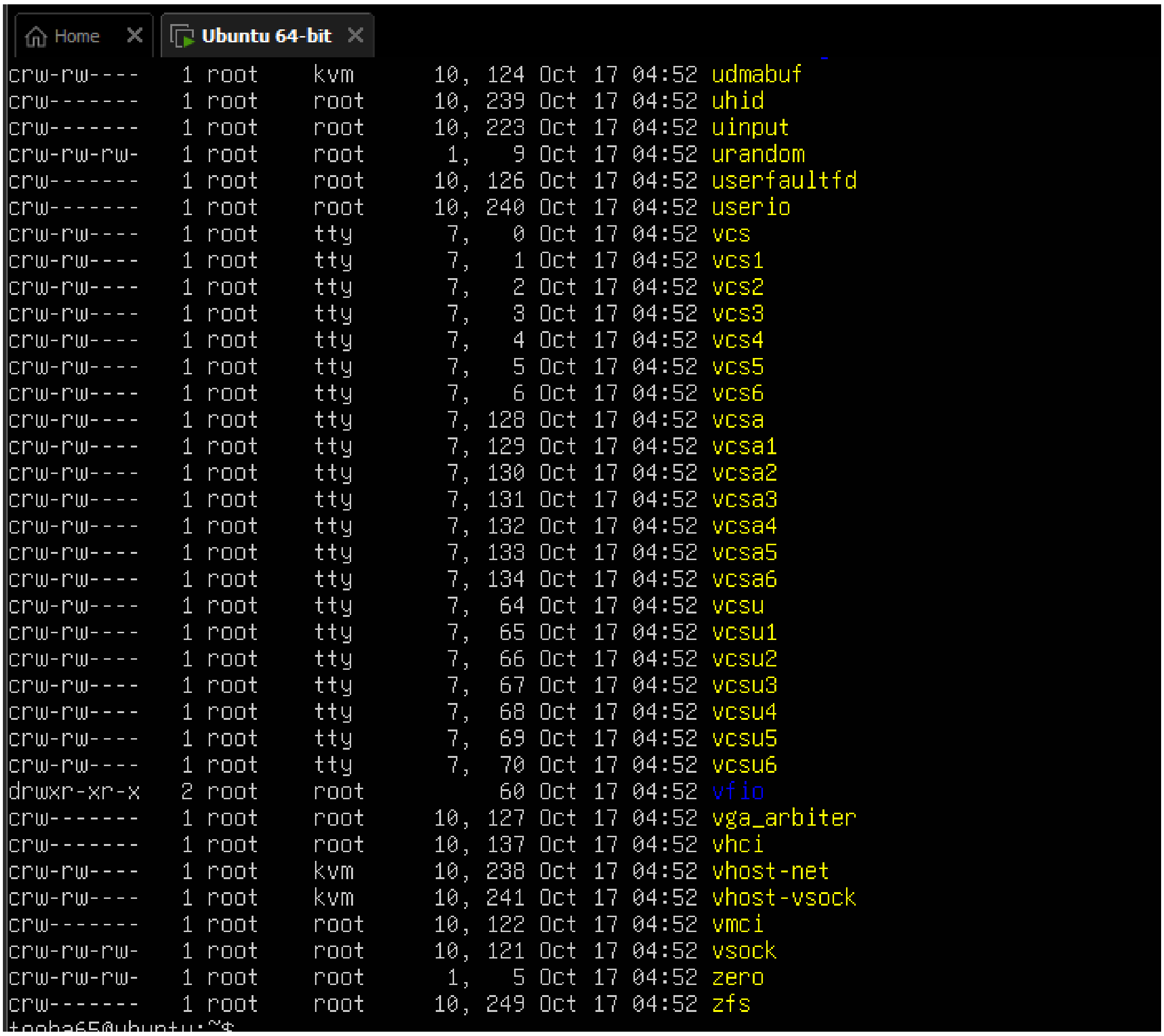
```
tooba65@ubuntu:~$ ls -la /opt
total 8
drwxr-xr-x  2 root root 4096 Aug  5 16:54 .
drwxr-xr-x 23 root root 4096 Oct  2 08:26 ..
tooba65@ubuntu:~$
```

ls -la /etc



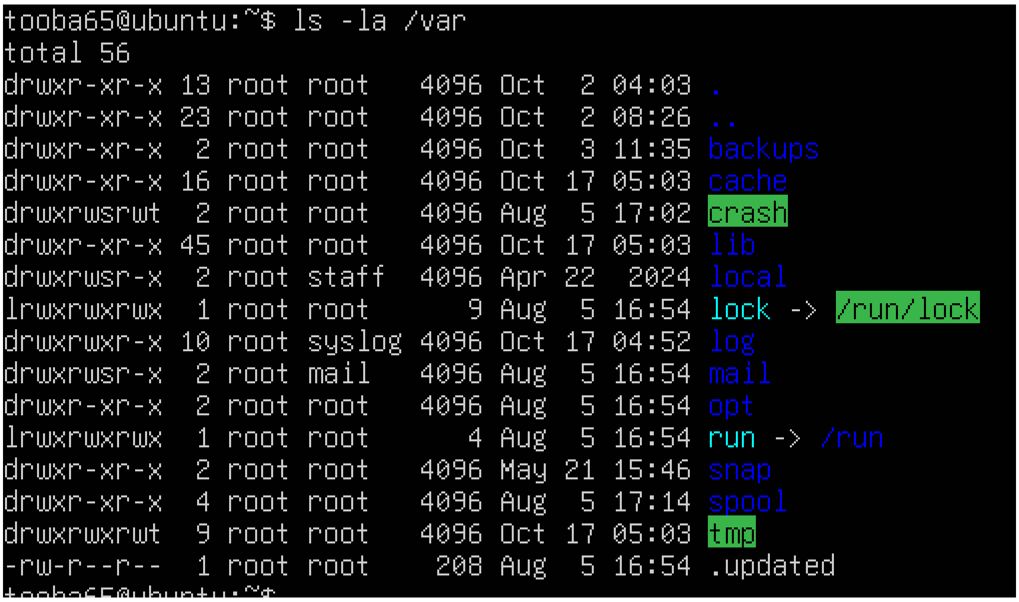
```
-rw-r--r--   1 root root       0 Aug  5 16:54 subuid-
-rw-r--r--   1 root root    4343 Jun 25 12:42 sudo.conf
-r--r-----   1 root root    1800 Jan 29  2024 sudoers
drwxr-xr-x   2 root root    4096 Aug  5 17:02 sudoers.d
-rw-r--r--   1 root root    9804 Jun 25 12:42 sudo_logsrvd.conf
drwxr-xr-x   2 root root    4096 Aug  5 17:14 supercat
-rw-r--r--   1 root root    2209 Mar 24  2024 sysctl.conf
drwxr-xr-x   2 root root    4096 Aug  5 17:02 sysctl.d
drwxr-xr-x   2 root root    4096 Aug  5 17:14 sysstat
drwxr-xr-x   6 root root    4096 Aug  5 16:49 systemd
drwxr-xr-x   2 root root    4096 Aug  5 17:00 terminfo
drwxr-xr-x   2 root root    4096 Oct  2 03:57 thermald
-rw-r--r--   1 root root       8 Aug  5 17:02 timezone
drwxr-xr-x   2 root root    4096 Aug  5 17:14 tmpfiles.d
drwxr-xr-x   2 root root    4096 Aug  5 17:14 ubuntu-advantage
-rw-r--r--   1 root root    1260 Jan 27  2023 ucf.conf
drwxr-xr-x   4 root root    4096 Aug  5 17:02 udev
drwxr-xr-x   2 root root    4096 Oct  2 04:00 udisks2
drwxr-xr-x   3 root root    4096 Aug  5 17:14 ufw
-rw-r--r--   1 root root     208 Aug  5 16:54 .updated
drwxr-xr-x   3 root root    4096 Aug  5 17:02 update-manager
drwxr-xr-x   2 root root    4096 Aug  5 17:14 update-motd.d
drwxr-xr-x   2 root root    4096 Aug  5 17:14 update-notifier
drwxr-xr-x   2 root root    4096 Oct  2 03:58 UPower
-rw-r--r--   1 root root    1523 Aug  5 17:14 usb_modeswitch.conf
drwxr-xr-x   2 root root    4096 Aug  5 17:14 usb_modeswitch.d
lrwxrwxrwx   1 root root      16 Aug  5 17:02 vconsole.conf -> default/keyboard
drwxr-xr-x   2 root root    4096 Oct  2 04:00 vim
drwxr-xr-x   4 root root    4096 Oct  2 04:00 vmware-tools
lrwxrwxrwx   1 root root      23 Feb 26  2024 vtrgb -> /etc/alternatives/vtrgb
-rw-r--r--   1 root root    4942 Aug  5 17:14 wgetrc
drwxr-xr-x   4 root root    4096 Aug  5 17:02 X11
-rw-r--r--   1 root root     681 Apr  8  2024 xattr.conf
drwxr-xr-x   4 root root    4096 Aug  5 17:02 xdg
drwxr-xr-x   2 root root    4096 Aug  5 17:02 xml
-rw-r--r--   1 root root     460 Aug  5 17:14 zsh_command_not_found
gabe65@ubuntu:~$
```

ls -la /dev



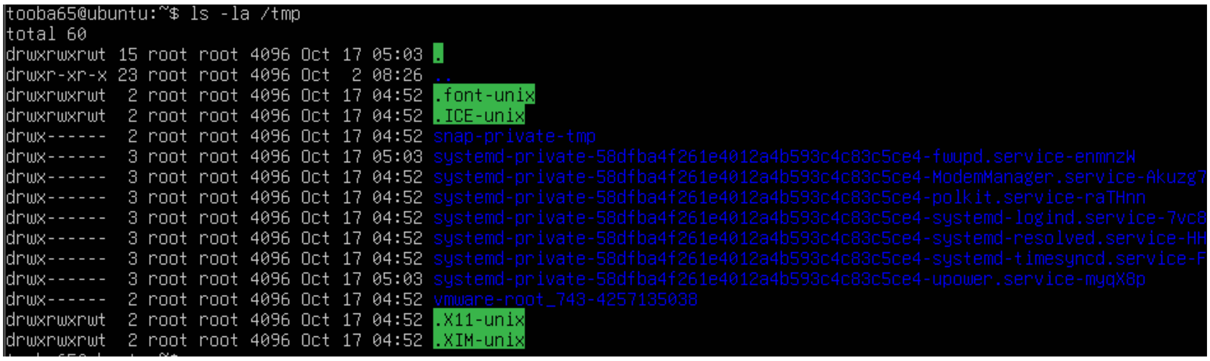
```
crw-rw----   1 root    kvm      10, 124 Oct 17 04:52 udmabuf
crw-------   1 root    root     10, 239 Oct 17 04:52 uhid
crw-------   1 root    root     10, 223 Oct 17 04:52 uinput
crw-rw-rw-   1 root    root      1,   9 Oct 17 04:52 urandom
crw-------   1 root    root     10, 126 Oct 17 04:52 userfaultfd
crw-------   1 root    root     10, 240 Oct 17 04:52 userio
crw-rw----   1 root    tty       7,   0 Oct 17 04:52 vcs
crw-rw----   1 root    tty       7,   1 Oct 17 04:52 vcs1
crw-rw----   1 root    tty       7,   2 Oct 17 04:52 vcs2
crw-rw----   1 root    tty       7,   3 Oct 17 04:52 vcs3
crw-rw----   1 root    tty       7,   4 Oct 17 04:52 vcs4
crw-rw----   1 root    tty       7,   5 Oct 17 04:52 vcs5
crw-rw----   1 root    tty       7,   6 Oct 17 04:52 vcs6
crw-rw----   1 root    tty       7, 128 Oct 17 04:52 vcsa
crw-rw----   1 root    tty       7, 129 Oct 17 04:52 vcsa1
crw-rw----   1 root    tty       7, 130 Oct 17 04:52 vcsa2
crw-rw----   1 root    tty       7, 131 Oct 17 04:52 vcsa3
crw-rw----   1 root    tty       7, 132 Oct 17 04:52 vcsa4
crw-rw----   1 root    tty       7, 133 Oct 17 04:52 vcsa5
crw-rw----   1 root    tty       7, 134 Oct 17 04:52 vcsa6
crw-rw----   1 root    tty       7,  64 Oct 17 04:52 vcsu
crw-rw----   1 root    tty       7,  65 Oct 17 04:52 vcsu1
crw-rw----   1 root    tty       7,  66 Oct 17 04:52 vcsu2
crw-rw----   1 root    tty       7,  67 Oct 17 04:52 vcsu3
crw-rw----   1 root    tty       7,  68 Oct 17 04:52 vcsu4
crw-rw----   1 root    tty       7,  69 Oct 17 04:52 vcsu5
crw-rw----   1 root    tty       7,  70 Oct 17 04:52 vcsu6
drwxr-xr-x   2 root    root          60 Oct 17 04:52 vfio
crw-------   1 root    root     10, 127 Oct 17 04:52 vga_arbiter
crw-------   1 root    root     10, 137 Oct 17 04:52 vhci
crw-rw----   1 root    kvm      10, 238 Oct 17 04:52 vhost-net
crw-rw----   1 root    kvm      10, 241 Oct 17 04:52 vhost-vsock
crw-------   1 root    root     10, 122 Oct 17 04:52 vmci
crw-rw-rw-   1 root    root     10, 121 Oct 17 04:52 vsock
crw-rw-rw-   1 root    root      1,   5 Oct 17 04:52 zero
crw-------   1 root    root     10, 249 Oct 17 04:52 zfs
tooba65@ubuntu:~$
```

ls -la /var



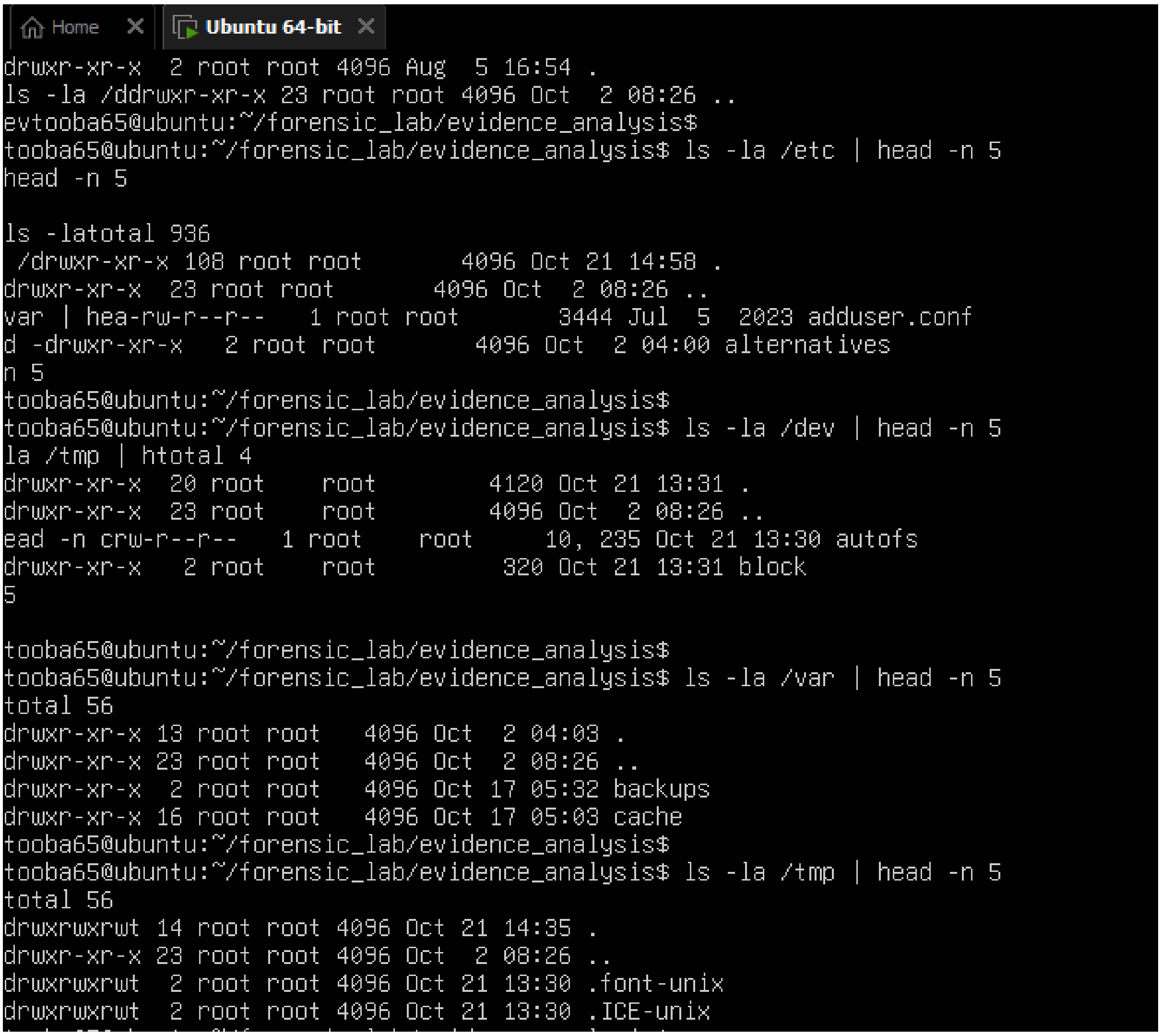
```
tooba65@ubuntu:~$ ls -la /var
total 56
drwxr-xr-x 13 root root   4096 Oct  2 04:03 .
drwxr-xr-x 23 root root   4096 Oct  2 08:26 ..
drwxr-xr-x  2 root root   4096 Oct  3 11:35 backups
drwxr-xr-x 16 root root   4096 Oct 17 05:03 cache
drwxrwsrwt  2 root root   4096 Aug  5 17:02 crash
drwxr-xr-x 45 root root   4096 Oct 17 05:03 lib
drwxrwsr-x  2 root staff  4096 Apr 22  2024 local
lrwxrwxrwx  1 root root      9 Aug  5 16:54 lock -> /run/lock
drwxrwxr-x 10 root syslog 4096 Oct 17 04:52 log
drwxrwsr-x  2 root mail   4096 Aug  5 16:54 mail
drwxr-xr-x  2 root root   4096 Aug  5 16:54 opt
lrwxrwxrwx  1 root root      4 Aug  5 16:54 run -> /run
drwxr-xr-x  2 root root   4096 May 21 15:46 snap
drwxr-xr-x  4 root root   4096 Aug  5 17:14 spool
drwxrwxrwt  9 root root   4096 Oct 17 05:03 tmp
-rw-r--r--  1 root root    208 Aug  5 16:54 .updated
tooba65@ubuntu:~$
```

ls -la /tmp



```
tooba65@ubuntu:~$ ls -la /tmp
total 60
drwxrwxrwt 15 root root 4096 Oct 17 05:03 .
drwxr-xr-x 23 root root 4096 Oct  2 08:26 ..
drwxrwxrwt  2 root root 4096 Oct 17 04:52 .font-unix
drwxrwxrwt  2 root root 4096 Oct 17 04:52 .ICE-unix
drwx------  2 root root 4096 Oct 17 04:52 snap-private-tmp
drwx------  3 root root 4096 Oct 17 05:03 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-fwupd.service-enmnzW
drwx------  3 root root 4096 Oct 17 04:52 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-ModemManager.service-Akuzg7
drwx------  3 root root 4096 Oct 17 04:52 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-polkit.service-raTHnn
drwx------  3 root root 4096 Oct 17 04:52 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-systemd-logind.service-7vc8
drwx------  3 root root 4096 Oct 17 04:52 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-systemd-resolved.service-HH
drwx------  3 root root 4096 Oct 17 04:52 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-systemd-timesyncd.service-F
drwx------  3 root root 4096 Oct 17 05:03 systemd-private-58dfba4f261e4012a4b593c4c83c5ce4-upower.service-myqX8p
drwx------  2 root root 4096 Oct 17 04:52 vmware-root_743-4257135038
drwxrwxrwt  2 root root 4096 Oct 17 04:52 .X11-unix
drwxrwxrwt  2 root root 4096 Oct 17 04:52 .XIM-unix
```

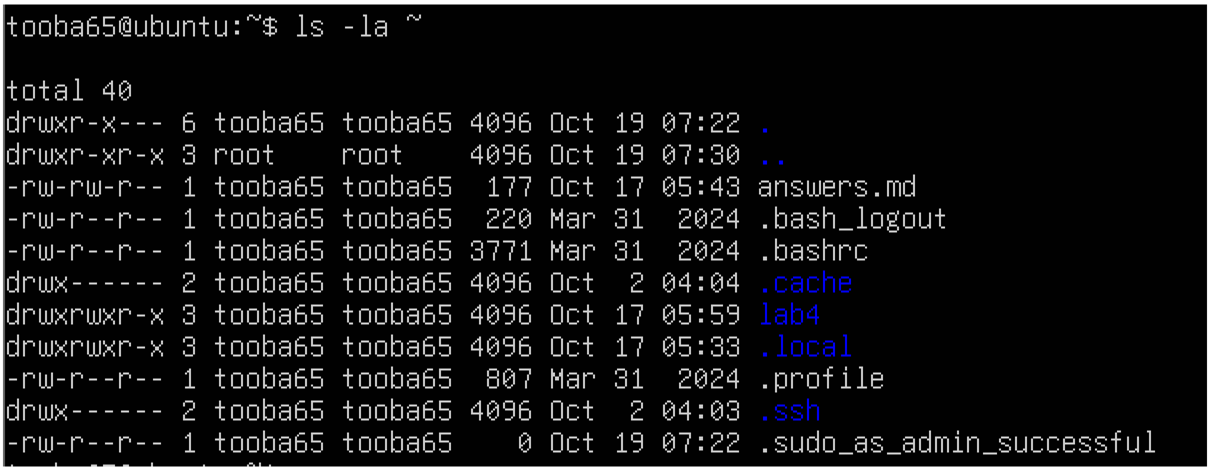
Here I print directory name + top few entries for each, all in one terminal view.



```
drwxr-xr-x  2 root root 4096 Aug  5 16:54 .
ls -la /ddrwxr-xr-x 23 root root 4096 Oct  2 08:26 ..
evtooba65@ubuntu:~/forensic_lab/evidence_analysis$
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ ls -la /etc | head -n 5
head -n 5

ls -latotal 936
 /drwxr-xr-x 108 root root        4096 Oct 21 14:58 .
drwxr-xr-x  23 root root        4096 Oct  2 08:26 ..
var | hea-rw-r--r--   1 root root        3444 Jul  5  2023 adduser.conf
d -drwxr-xr-x   2 root root        4096 Oct  2 04:00 alternatives
n 5
tooba65@ubuntu:~/forensic_lab/evidence_analysis$
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ ls -la /dev | head -n 5
la /tmp | htotal 4
drwxr-xr-x  20 root    root         4120 Oct 21 13:31 .
drwxr-xr-x  23 root    root         4096 Oct  2 08:26 ..
ead -n crw-r--r--   1 root    root      10, 235 Oct 21 13:30 autofs
drwxr-xr-x   2 root    root          320 Oct 21 13:31 block
5

tooba65@ubuntu:~/forensic_lab/evidence_analysis$
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ ls -la /var | head -n 5
total 56
drwxr-xr-x 13 root root   4096 Oct  2 04:03 .
drwxr-xr-x 23 root root   4096 Oct  2 08:26 ..
drwxr-xr-x  2 root root   4096 Oct 17 05:32 backups
drwxr-xr-x 16 root root   4096 Oct 17 05:03 cache
tooba65@ubuntu:~/forensic_lab/evidence_analysis$
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ ls -la /tmp | head -n 5
total 56
drwxrwxrwt 14 root root 4096 Oct 21 14:35 .
drwxr-xr-x 23 root root 4096 Oct  2 08:26 ..
drwxrwxrwt  2 root root 4096 Oct 21 13:30 .font-unix
drwxrwxrwt  2 root root 4096 Oct 21 13:30 .ICE-unix
```

4. Display all hidden files in your home directory.

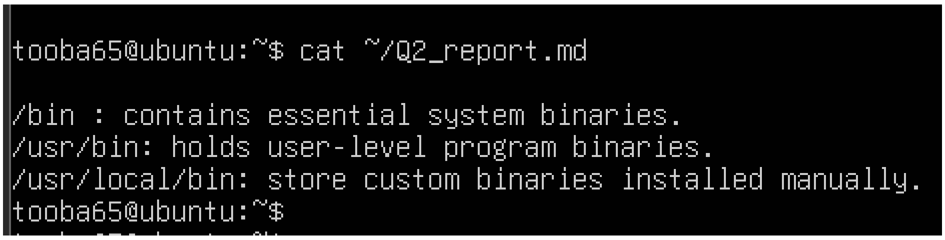
   ○ Screenshot as Q2_hidden_files.png



```
tooba65@ubuntu:~$ ls -la ~

total 40
drwxr-x--- 6 tooba65 tooba65 4096 Oct 19 07:22 .
drwxr-xr-x 3 root    root    4096 Oct 19 07:30 ..
-rw-rw-r-- 1 tooba65 tooba65  177 Oct 17 05:43 answers.md
-rw-r--r-- 1 tooba65 tooba65  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 tooba65 tooba65 3771 Mar 31  2024 .bashrc
drwx------ 2 tooba65 tooba65 4096 Oct  2 04:04 .cache
drwxrwxr-x 3 tooba65 tooba65 4096 Oct 17 05:59 lab4
drwxrwxr-x 3 tooba65 tooba65 4096 Oct 17 05:33 .local
-rw-r--r-- 1 tooba65 tooba65  807 Mar 31  2024 .profile
drwx------ 2 tooba65 tooba65 4096 Oct  2 04:03 .ssh
-rw-r--r-- 1 tooba65 tooba65    0 Oct 19 07:22 .sudo_as_admin_successful
```

5. Create a markdown file summarizing your findings on key binary directories.

   ○ Screenshot as Q2_report_file.png



```
tooba65@ubuntu:~$ cat ~/Q2_report.md

/bin : contains essential system binaries.
/usr/bin: holds user-level program binaries.
/usr/local/bin: store custom binaries installed manually.
tooba65@ubuntu:~$
```

---

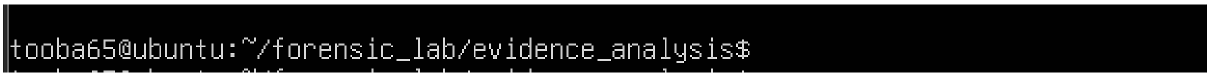
3. Evidence Handling & File Operations

Scenario:
You are creating a sandbox environment to safely analyze and handle suspicious files collected from a compromised system.

Steps:

1. Create a structured folder hierarchy under your home directory for analysis.

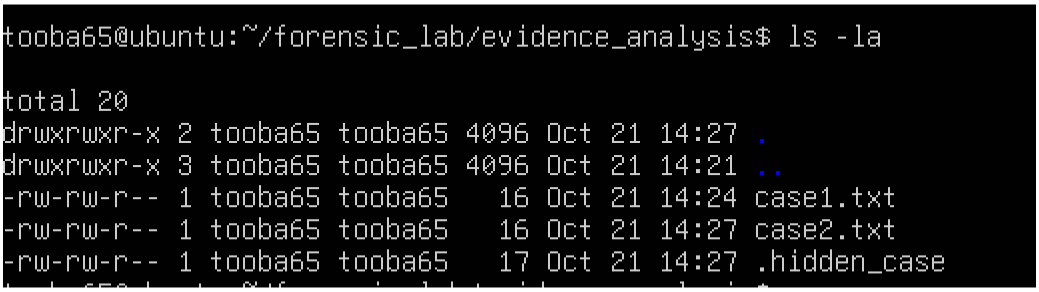
   ○ Screenshot as Q3_workspace_created.png



```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$
```

2. Create three text files, including one hidden file, in your workspace.

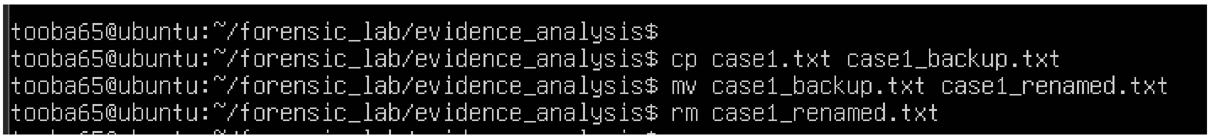
   ○ Screenshot as Q3_files_created.png



```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ ls -la

total 20
drwxrwxr-x 2 tooba65 tooba65 4096 Oct 21 14:27 .
drwxrwxr-x 3 tooba65 tooba65 4096 Oct 21 14:21 ..
-rw-rw-r-- 1 tooba65 tooba65   16 Oct 21 14:24 case1.txt
-rw-rw-r-- 1 tooba65 tooba65   16 Oct 21 14:27 case2.txt
-rw-rw-r-- 1 tooba65 tooba65   17 Oct 21 14:27 .hidden_case
```

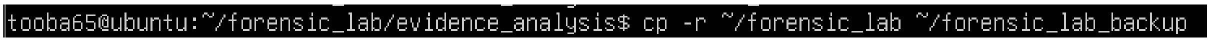
3. Create a backup copy of one file, rename it, and then delete it after verification.

- Screenshot as Q3_backup_handling.png



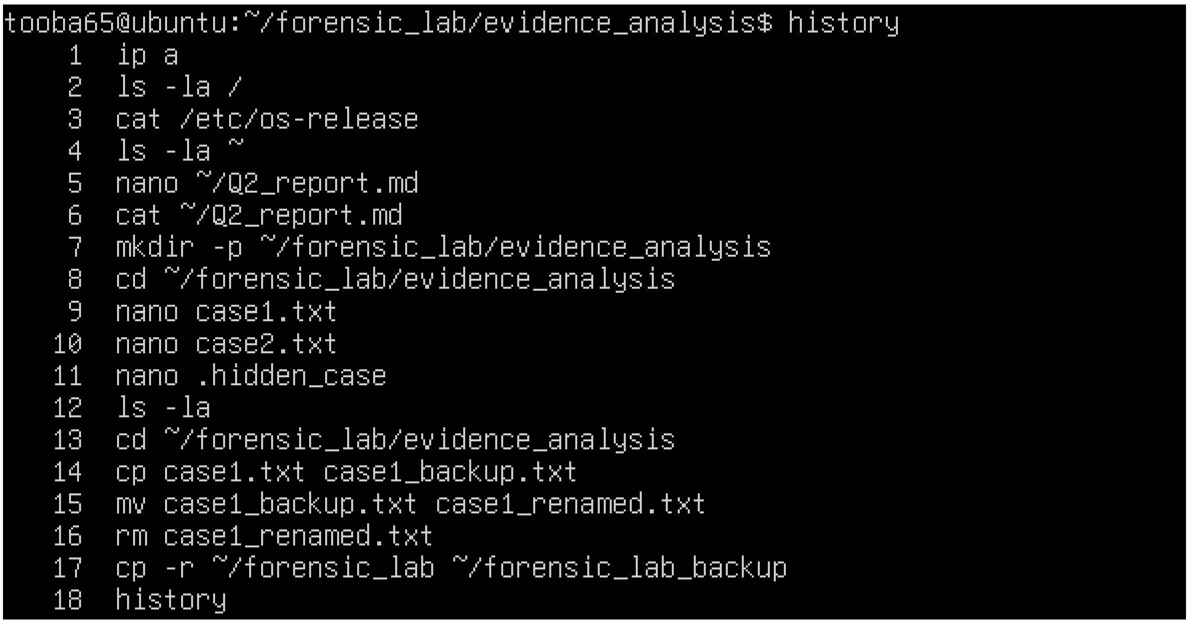
```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ cp case1.txt case1_backup.txt
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ mv case1_backup.txt case1_renamed.txt
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ rm case1_renamed.txt
```

4. Copy the entire workspace as an evidence backup folder.
   - Screenshot as Q3_workspace_backup.png



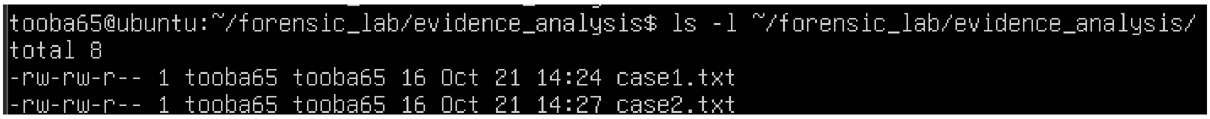
```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ cp -r ~/forensic_lab ~/forensic_lab_backup
```

5. Display your command history to document all actions performed.
   - Screenshot as Q3_command_history.png



```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ history
    1  ip a
    2  ls -la /
    3  cat /etc/os-release
    4  ls -la ~
    5  nano ~/Q2_report.md
    6  cat ~/Q2_report.md
    7  mkdir -p ~/forensic_lab/evidence_analysis
    8  cd ~/forensic_lab/evidence_analysis
    9  nano case1.txt
   10  nano case2.txt
   11  nano .hidden_case
   12  ls -la
   13  cd ~/forensic_lab/evidence_analysis
   14  cp case1.txt case1_backup.txt
   15  mv case1_backup.txt case1_renamed.txt
   16  rm case1_renamed.txt
   17  cp -r ~/forensic_lab ~/forensic_lab_backup
   18  history
```

6. Demonstrate Linux auto-completion by typing a partial command or filename.
   - Screenshot as Q3_autocomplete.png



```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ ls -l ~/forensic_lab/evidence_analysis/
total 8
-rw-rw-r-- 1 tooba65 tooba65 16 Oct 21 14:24 case1.txt
-rw-rw-r-- 1 tooba65 tooba65 16 Oct 21 14:27 case2.txt
```

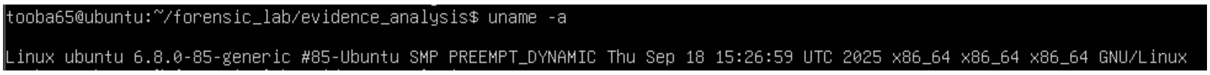
---

4. System Profiling and Process Monitoring

Scenario:
You are investigating a potential malware infection that is consuming excessive resources on the Linux VM.

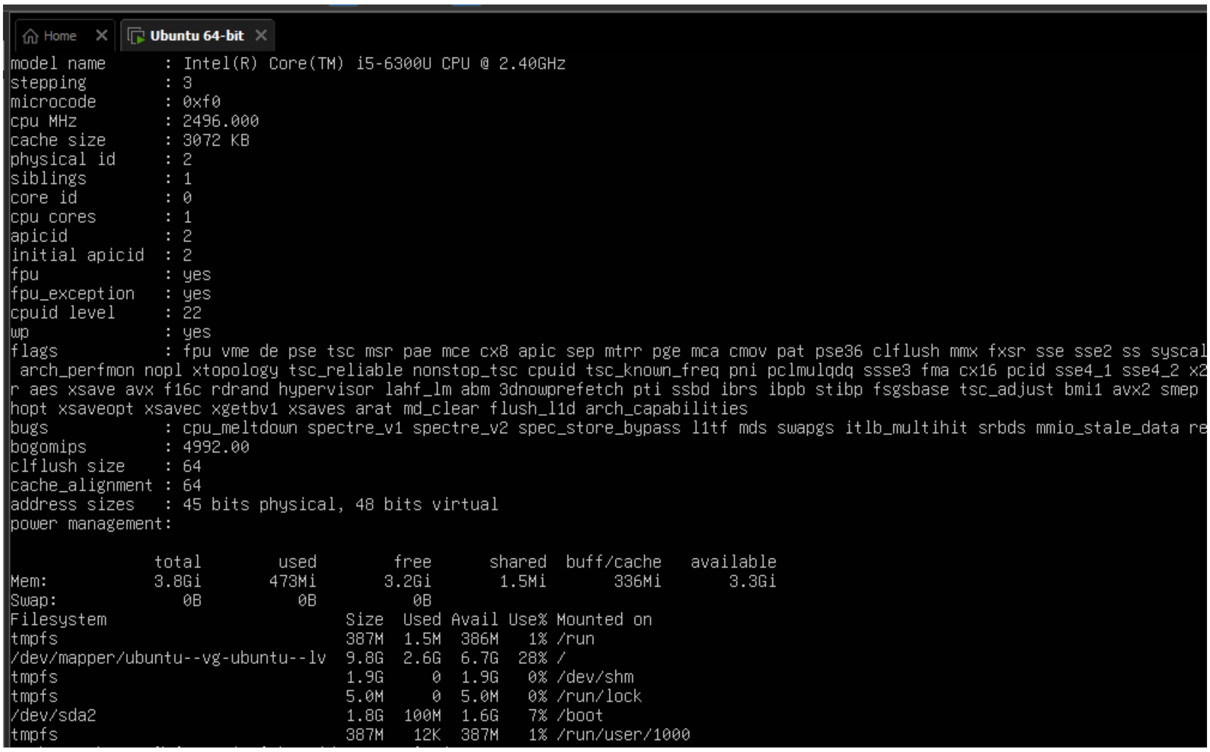
Steps:

1. Display the system's OS and kernel version for the investigation report.
   - Screenshot as Q4_system_info.png



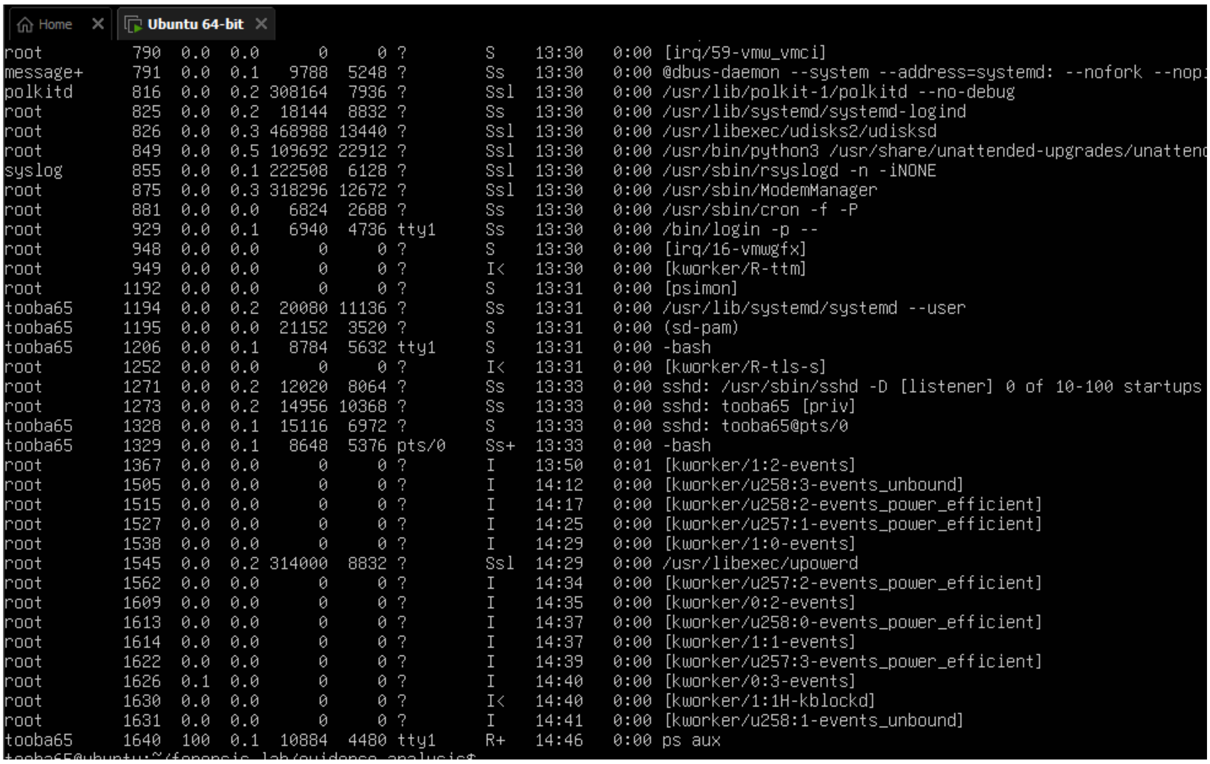
```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ uname -a

Linux ubuntu 6.8.0-85-generic #85-Ubuntu SMP PREEMPT_DYNAMIC Thu Sep 18 15:26:59 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
```

2. Display CPU, memory, and disk usage information.
   - Screenshot as Q4_resource_info.png



```
model name      : Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
stepping        : 3
microcode       : 0xf0
cpu MHz         : 2496.000
cache size      : 3072 KB
physical id     : 2
siblings        : 1
core id         : 0
cpu cores       : 1
apicid          : 2
initial apicid  : 2
fpu             : yes
fpu_exception   : yes
cpuid level     : 22
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscal
 arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2
r aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep
hopt xsaveopt xsavec xgetbv1 xsaves arat md_clear flush_l1d arch_capabilities
bugs            : cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf mds swapgs itlb_multihit srbds mmio_stale_data re
bogomips        : 4992.00
clflush size    : 64
cache_alignment : 64
address sizes   : 45 bits physical, 48 bits virtual
power management:

               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       473Mi       3.2Gi       1.5Mi       336Mi       3.3Gi
Swap:             0B          0B          0B
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              387M  1.5M  386M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  9.8G  2.6G  6.7G  28% /
tmpfs                              1.9G     0  1.9G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          1.8G  100M  1.6G   7% /boot
tmpfs                              387M   12K  387M   1% /run/user/1000
```

3. Display all active running processes to identify suspicious activity.
   - Screenshot as Q4_process_list.png



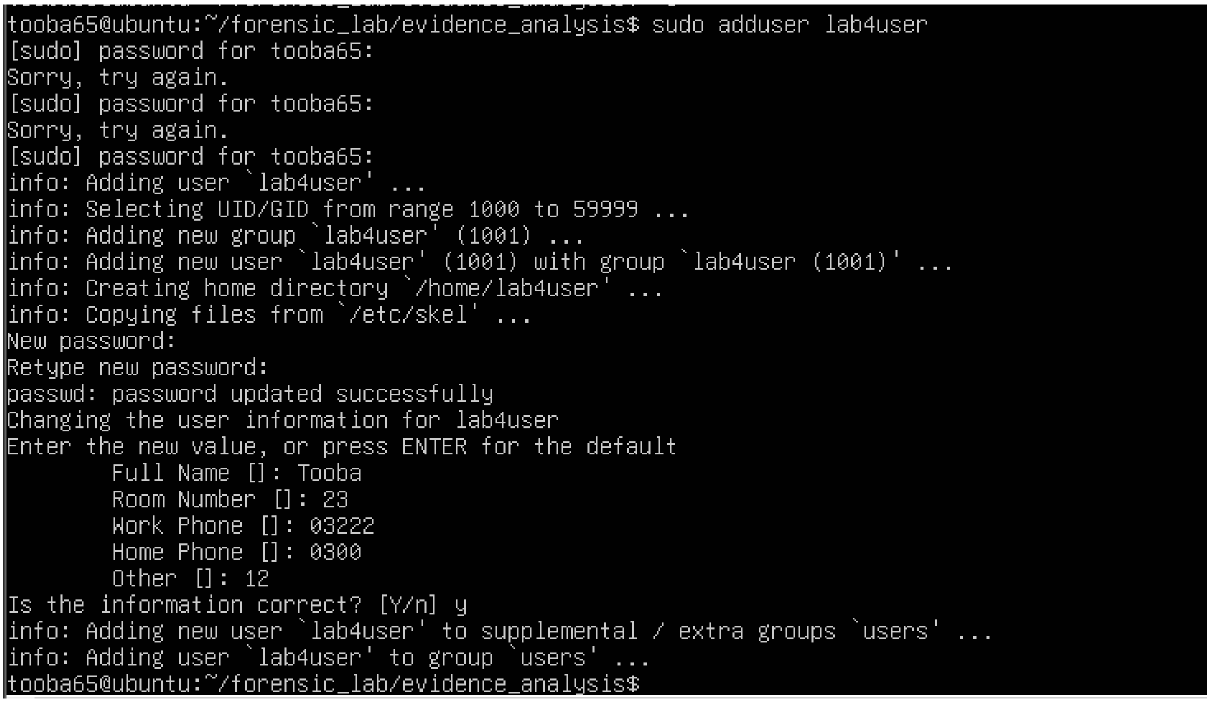
```
root         790  0.0  0.0      0     0 ?        S    13:30   0:00 [irq/59-vmw_vmci]
message+     791  0.0  0.1   9788  5248 ?        Ss   13:30   0:00 @dbus-daemon --system --address=systemd: --nofork --nop
polkitd      816  0.0  0.2 308164  7936 ?        Ssl  13:30   0:00 /usr/lib/polkit-1/polkitd --no-debug
root         825  0.0  0.2  18144  8832 ?        Ss   13:30   0:00 /usr/lib/systemd/systemd-logind
root         826  0.0  0.3 468988 13440 ?        Ssl  13:30   0:00 /usr/libexec/udisks2/udisksd
root         849  0.0  0.5 109692 22912 ?        Ssl  13:30   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattend
syslog       855  0.0  0.1 222508  6128 ?        Ssl  13:30   0:00 /usr/sbin/rsyslogd -n -iNONE
root         875  0.0  0.3 318296 12672 ?        Ssl  13:30   0:00 /usr/sbin/ModemManager
root         881  0.0  0.0   6824  2688 ?        Ss   13:30   0:00 /usr/sbin/cron -f -P
root         929  0.0  0.1   6940  4736 tty1     Ss   13:30   0:00 /bin/login -p --
root         948  0.0  0.0      0     0 ?        S    13:30   0:00 [irq/16-vmwgfx]
root         949  0.0  0.0      0     0 ?        I<   13:30   0:00 [kworker/R-ttm]
root        1192  0.0  0.0      0     0 ?        S    13:31   0:00 [psimon]
tooba65     1194  0.0  0.2  20080 11136 ?        Ss   13:31   0:00 /usr/lib/systemd/systemd --user
tooba65     1195  0.0  0.0  21152  3520 ?        S    13:31   0:00 (sd-pam)
tooba65     1206  0.0  0.1   8784  5632 tty1     S    13:31   0:00 -bash
root        1252  0.0  0.0      0     0 ?        I<   13:31   0:00 [kworker/R-tls-s]
root        1271  0.0  0.2  12020  8064 ?        Ss   13:33   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        1273  0.0  0.2  14956 10368 ?        Ss   13:33   0:00 sshd: tooba65 [priv]
tooba65     1328  0.0  0.1  15116  6972 ?        S    13:33   0:00 sshd: tooba65@pts/0
tooba65     1329  0.0  0.1   8648  5376 pts/0    Ss+  13:33   0:00 -bash
root        1367  0.0  0.0      0     0 ?        I    13:50   0:01 [kworker/1:2-events]
root        1505  0.0  0.0      0     0 ?        I    14:12   0:00 [kworker/u258:3-events_unbound]
root        1515  0.0  0.0      0     0 ?        I    14:17   0:00 [kworker/u258:2-events_power_efficient]
root        1527  0.0  0.0      0     0 ?        I    14:25   0:00 [kworker/u257:1-events_power_efficient]
root        1538  0.0  0.0      0     0 ?        I    14:29   0:00 [kworker/1:0-events]
root        1545  0.0  0.2 314000  8832 ?        Ssl  14:29   0:00 /usr/libexec/upowerd
root        1562  0.0  0.0      0     0 ?        I    14:34   0:00 [kworker/u257:2-events_power_efficient]
root        1609  0.0  0.0      0     0 ?        I    14:35   0:00 [kworker/0:2-events]
root        1613  0.0  0.0      0     0 ?        I    14:37   0:00 [kworker/u258:0-events_power_efficient]
root        1614  0.0  0.0      0     0 ?        I    14:37   0:00 [kworker/1:1-events]
root        1622  0.0  0.0      0     0 ?        I    14:39   0:00 [kworker/u257:3-events_power_efficient]
root        1626  0.1  0.0      0     0 ?        I    14:40   0:00 [kworker/0:3-events]
root        1630  0.0  0.0      0     0 ?        I<   14:40   0:00 [kworker/1:1H-kblockd]
root        1631  0.0  0.0      0     0 ?        I    14:41   0:00 [kworker/u258:1-events_unbound]
tooba65     1640  100  0.1  10884  4480 tty1     R+   14:46   0:00 ps aux
tooba65@ubuntu:~/forensic_lab/evidence_analysis$
```

5. User Account Audit & Privilege Escalation Simulation

Scenario:
You are performing a **user activity audit** on a compromised Linux server.
The SOC suspects a newly created account (lab4user) may have been used for unauthorized access.
Your task is to simulate the account creation, perform privilege tests, and analyze authentication logs for forensic evidence.

Steps:

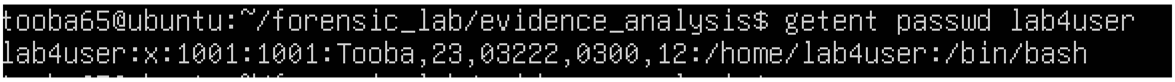
1. Create a new test user named lab4user.
   - Screenshot as Q5_user_created.png



```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ sudo adduser lab4user
[sudo] password for tooba65:
Sorry, try again.
[sudo] password for tooba65:
Sorry, try again.
[sudo] password for tooba65:
info: Adding user `lab4user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lab4user' (1001) ...
info: Adding new user `lab4user' (1001) with group `lab4user (1001)' ...
info: Creating home directory `/home/lab4user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lab4user
Enter the new value, or press ENTER for the default
        Full Name []: Tooba
        Room Number []: 23
        Work Phone []: 03222
        Home Phone []: 0300
        Other []: 12
Is the information correct? [Y/n] y
info: Adding new user `lab4user' to supplemental / extra groups `users' ...
info: Adding user `lab4user' to group `users' ...
tooba65@ubuntu:~/forensic_lab/evidence_analysis$
```

2. Verify that the new user record exists in the system's user database.

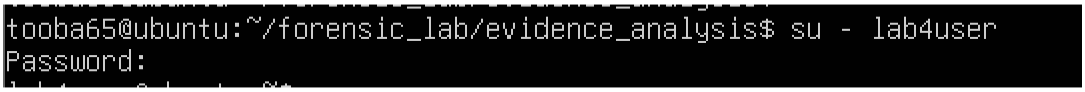
   ○ Screenshot as Q5_user_verified.png



```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ getent passwd lab4user
lab4user:x:1001:1001:Tooba,23,03222,0300,12:/home/lab4user:/bin/bash
```

3. Log in as lab4user and confirm successful login.

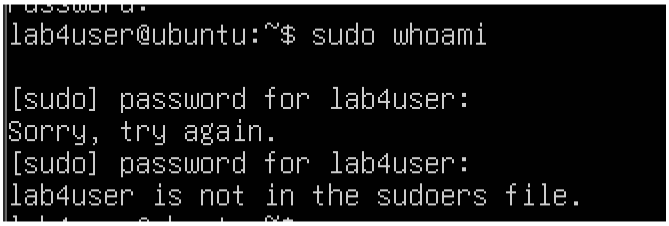
   ○ Screenshot as Q5_user_login.png



```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ su - lab4user
Password:
```

4. Attempt to run an administrative command as lab4user (expect permission denied).

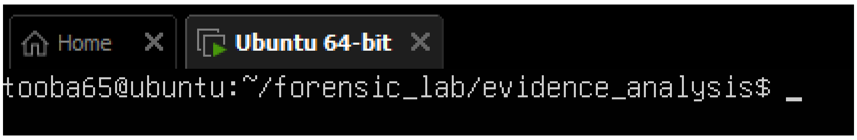
   ○ Screenshot as Q5_permission_denied.png



```
lab4user@ubuntu:~$ sudo whoami

[sudo] password for lab4user:
Sorry, try again.
[sudo] password for lab4user:
lab4user is not in the sudoers file.
```

5. Switch back to your main analyst account.

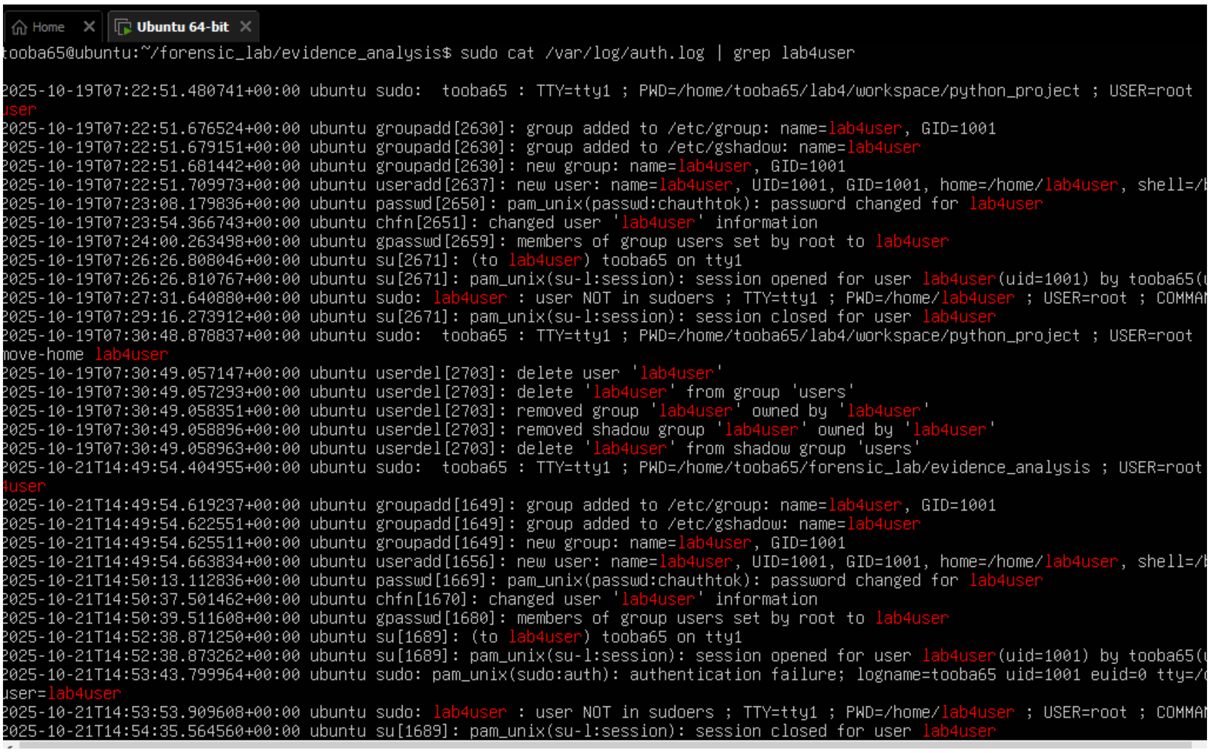
   ○ Screenshot as Q5_switch_back.png



```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ _
```

6. Inspect the system authentication logs located at /var/log/auth.log to determine whether the lab4user account attempted any logins (successful or failed).

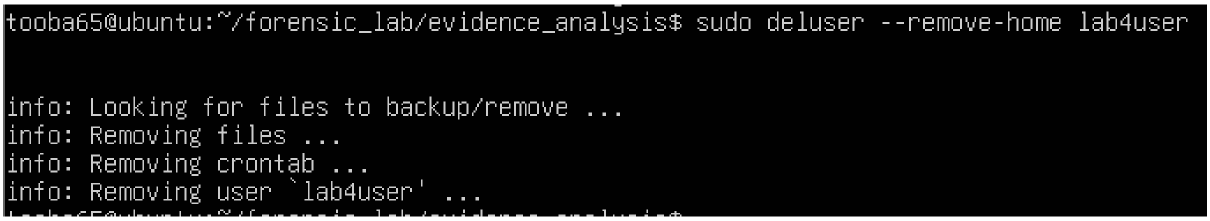
   - ○ Screenshot as Q5_authlog_analysis.png



```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ sudo cat /var/log/auth.log | grep lab4user

2025-10-19T07:22:51.480741+00:00 ubuntu sudo:  tooba65 : TTY=tty1 ; PWD=/home/tooba65/lab4/workspace/python_project ; USER=root
user
2025-10-19T07:22:51.676524+00:00 ubuntu groupadd[2630]: group added to /etc/group: name=lab4user, GID=1001
2025-10-19T07:22:51.679151+00:00 ubuntu groupadd[2630]: group added to /etc/gshadow: name=lab4user
2025-10-19T07:22:51.681442+00:00 ubuntu groupadd[2630]: new group: name=lab4user, GID=1001
2025-10-19T07:22:51.709973+00:00 ubuntu useradd[2637]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4user, shell=/
2025-10-19T07:23:08.179836+00:00 ubuntu passwd[2650]: pam_unix(passwd:chauthtok): password changed for lab4user
2025-10-19T07:23:54.366743+00:00 ubuntu chfn[2651]: changed user 'lab4user' information
2025-10-19T07:24:00.263498+00:00 ubuntu gpasswd[2659]: members of group users set by root to lab4user
2025-10-19T07:26:26.808046+00:00 ubuntu su[2671]: (to lab4user) tooba65 on tty1
2025-10-19T07:26:26.810767+00:00 ubuntu su[2671]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by tooba65(
2025-10-19T07:27:31.640880+00:00 ubuntu sudo: lab4user : user NOT in sudoers ; TTY=tty1 ; PWD=/home/lab4user ; USER=root ; COMMAN
2025-10-19T07:29:16.273912+00:00 ubuntu su[2671]: pam_unix(su-l:session): session closed for user lab4user
2025-10-19T07:30:48.878837+00:00 ubuntu sudo:  tooba65 : TTY=tty1 ; PWD=/home/tooba65/lab4/workspace/python_project ; USER=root
move-home lab4user
2025-10-19T07:30:49.057147+00:00 ubuntu userdel[2703]: delete user 'lab4user'
2025-10-19T07:30:49.057293+00:00 ubuntu userdel[2703]: delete 'lab4user' from group 'users'
2025-10-19T07:30:49.058351+00:00 ubuntu userdel[2703]: removed group 'lab4user' owned by 'lab4user'
2025-10-19T07:30:49.058896+00:00 ubuntu userdel[2703]: removed shadow group 'lab4user' owned by 'lab4user'
2025-10-19T07:30:49.058963+00:00 ubuntu userdel[2703]: delete 'lab4user' from shadow group 'users'
2025-10-21T14:49:54.404955+00:00 ubuntu sudo:  tooba65 : TTY=tty1 ; PWD=/home/tooba65/forensic_lab/evidence_analysis ; USER=root
4user
2025-10-21T14:49:54.619237+00:00 ubuntu groupadd[1649]: group added to /etc/group: name=lab4user, GID=1001
2025-10-21T14:49:54.622551+00:00 ubuntu groupadd[1649]: group added to /etc/gshadow: name=lab4user
2025-10-21T14:49:54.625511+00:00 ubuntu groupadd[1649]: new group: name=lab4user, GID=1001
2025-10-21T14:49:54.663834+00:00 ubuntu useradd[1656]: new user: name=lab4user, UID=1001, GID=1001, home=/home/lab4user, shell=/
2025-10-21T14:50:13.112836+00:00 ubuntu passwd[1669]: pam_unix(passwd:chauthtok): password changed for lab4user
2025-10-21T14:50:37.501462+00:00 ubuntu chfn[1670]: changed user 'lab4user' information
2025-10-21T14:50:39.511608+00:00 ubuntu gpasswd[1680]: members of group users set by root to lab4user
2025-10-21T14:52:38.871250+00:00 ubuntu su[1689]: (to lab4user) tooba65 on tty1
2025-10-21T14:52:38.873262+00:00 ubuntu su[1689]: pam_unix(su-l:session): session opened for user lab4user(uid=1001) by tooba65(
2025-10-21T14:53:43.799964+00:00 ubuntu sudo: pam_unix(sudo:auth): authentication failure; logname=tooba65 uid=1001 euid=0 tty=/
user=lab4user
2025-10-21T14:53:53.909608+00:00 ubuntu sudo: lab4user : user NOT in sudoers ; TTY=tty1 ; PWD=/home/lab4user ; USER=root ; COMMAN
2025-10-21T14:54:35.564560+00:00 ubuntu su[1689]: pam_unix(su-l:session): session closed for user lab4user
```

7. (Optional) Remove the lab4user account after the audit and verify deletion.

   - ○ Screenshot as Q5_user_removed.png



```
tooba65@ubuntu:~/forensic_lab/evidence_analysis$ sudo deluser --remove-home lab4user


info: Looking for files to backup/remove ...
info: Removing files ...
info: Removing crontab ...
info: Removing user `lab4user' ...
tooba65@ubuntu:~/forensic_lab/evidence_analysis$
```