# **Linux System Administration Class Tasks**

# **Task 1: Search and Highlight the Word "error" in a Log File**

## Step 1: Create a Sample Log File

**Command:**

cat <<EOF > syslog.txt

Jan 30 10:23:01 server systemd: Started Session 1 of user root.

Jan 30 10:23:15 server sshd[1354]: error: PAM: Authentication failure for root from 192.168.1.5

Jan 30 10:23:20 server sshd[1354]: Accepted password for root from 192.168.1.5 port 22 ssh2

EOF

**Explanation:**  
This creates a file named syslog.txt with simulated system log entries, including one that contains the word error.

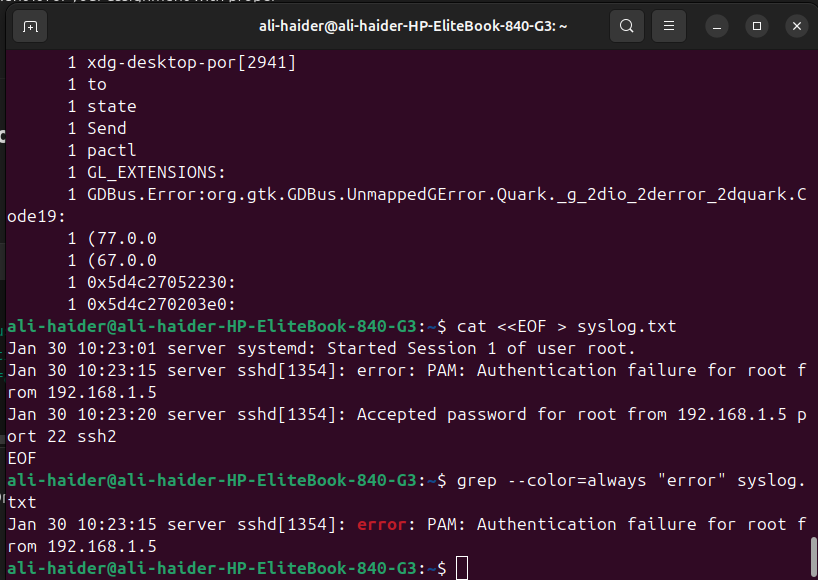
## Step 2: Search and Highlight the Word "error"

**Command:**

grep --color=always "error" syslog.txt

**Explanation:**  
This command searches for the word error and highlights it in the output using terminal colors.

**Output:**



# **Task 2: Use Regex to Match "fail" or "denied" in a Log File**

## Step 1: Create a Sample auth.log File

**Command:**

cat <<EOF > auth.log

Jan 30 11:12:01 server sshd[2001]: Failed password for invalid user test from 10.0.0.1 port 54720 ssh2

Jan 30 11:12:03 server sshd[2001]: Connection closed by 10.0.0.1 port 54720 [preauth]

Jan 30 11:12:05 server sshd[2002]: Access denied for user admin from 10.0.0.2

EOF

**Explanation:**  
This creates a file named auth.log with simulated authentication log entries containing the words Failed and denied.

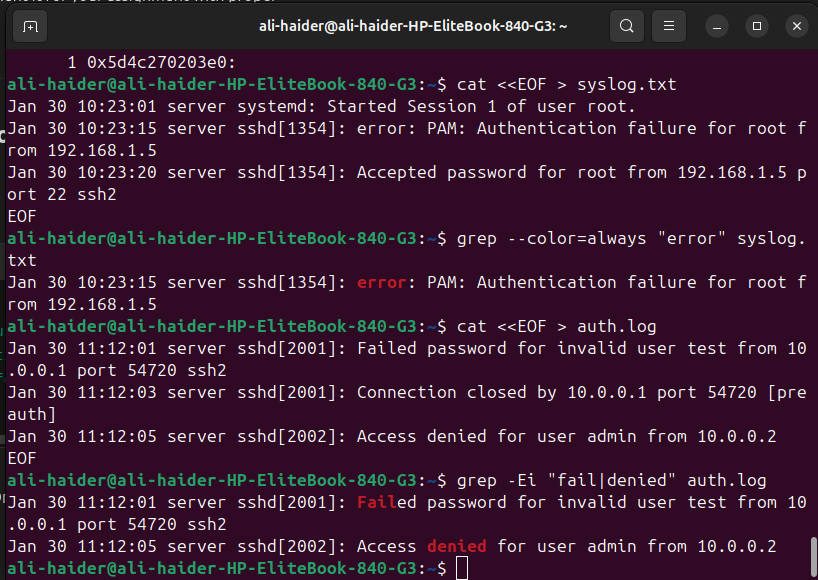
## Step 2: Use Regex to Match "fail" or "denied"

**Command:**

grep -Ei "fail|denied" auth.log

**Explanation:**  
This command searches the file using a case-insensitive regular expression to match either "fail" or "denied".

**Output:**



# **Linux System Administration Assignment**

## **Part 1: User & Group Permissions**

### **Task 1.1 – Create Users & Groups**

**Commands:**

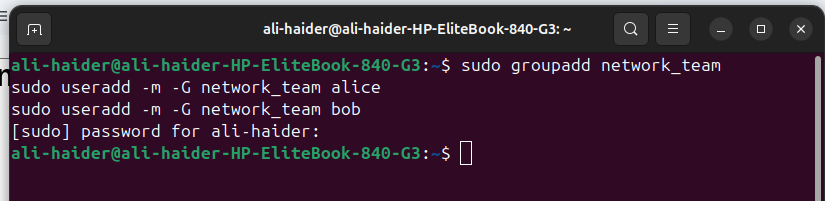
sudo groupadd network\_team

sudo useradd -m -G network\_team alice

sudo useradd -m -G network\_team bob

**Explanation:** Creates a group network\_team, adds users alice and bob to it.

**Output:**



### **Task 1.2 – Set Directory Permissions**

**Commands:**

sudo mkdir /opt/network\_data

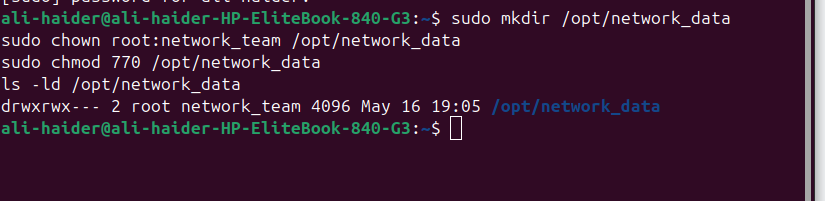
sudo chown root:network\_team /opt/network\_data

sudo chmod 770 /opt/network\_data

ls -ld /opt/network\_data

**Explanation:** Creates a shared directory for the group with read/write/execute permissions.

**Output:**



## **Part 2: Network Tools & Real-Time Checks**

### **Task 2.1 – Check Connectivity to google.com**

**Commands:**

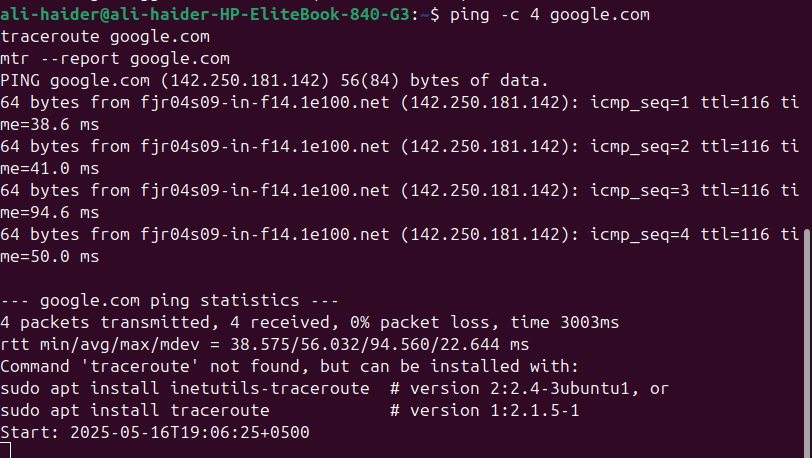
ping -c 4 google.com

traceroute google.com

mtr --report google.com

**Explanation:** Tests connectivity and routes to Google.

**Output:**



### **Task 2.2 – Check Open Ports & Listening Services**

**Commands:**

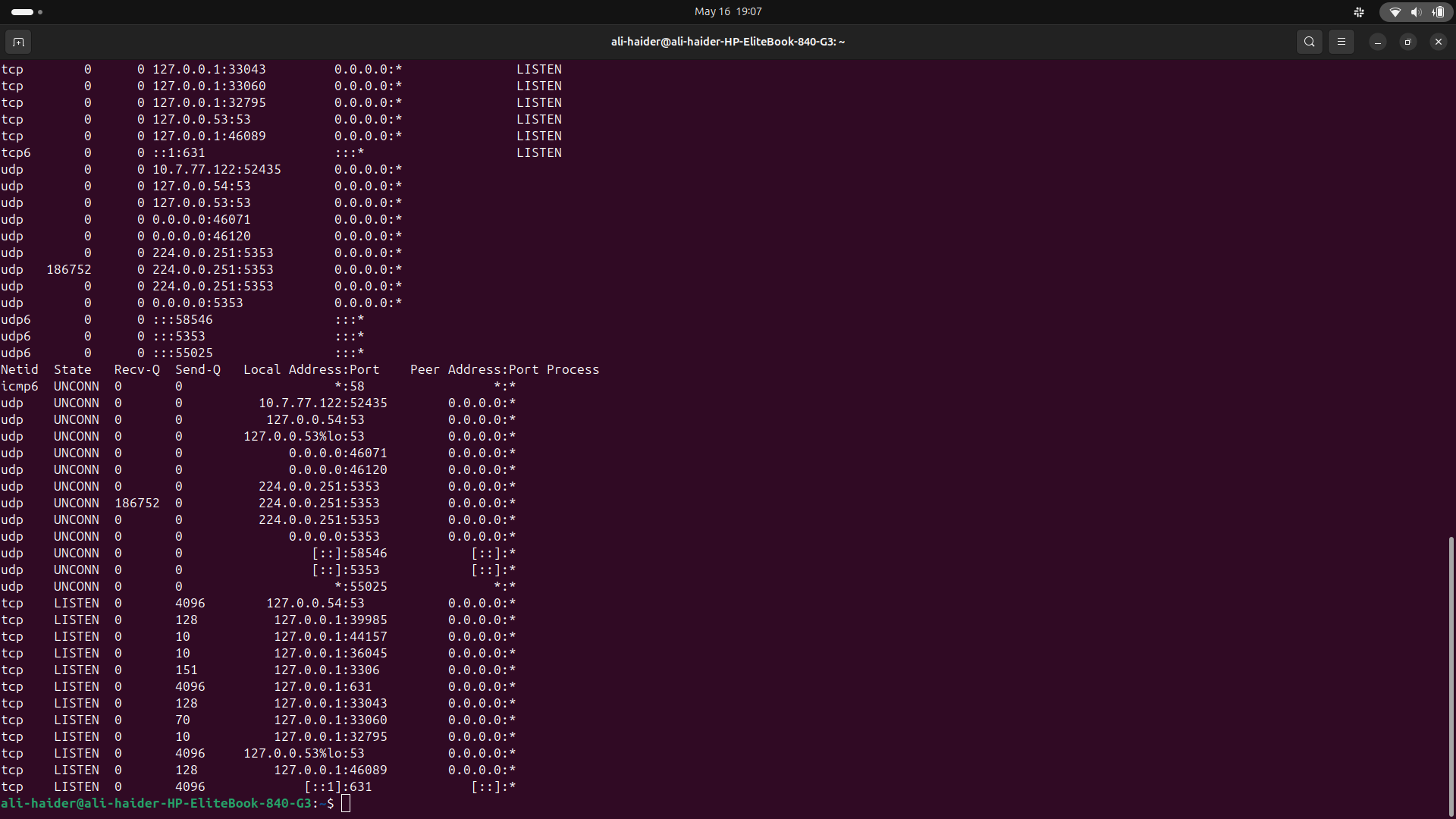
sudo apt install net-tools

sudo netstat -tuln

sudo ss -tulwn

**Explanation:** Lists open ports and listening services.

**Output:**



### **Task 2.3 – Test Remote Port Connectivity**

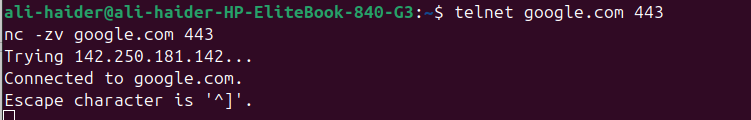
**Commands:**

telnet google.com 443

nc -zv google.com 443

**Explanation:** Checks if port 443 is open and accessible.

**Output:**



### **Task 2.4 – Check Network Interfaces**

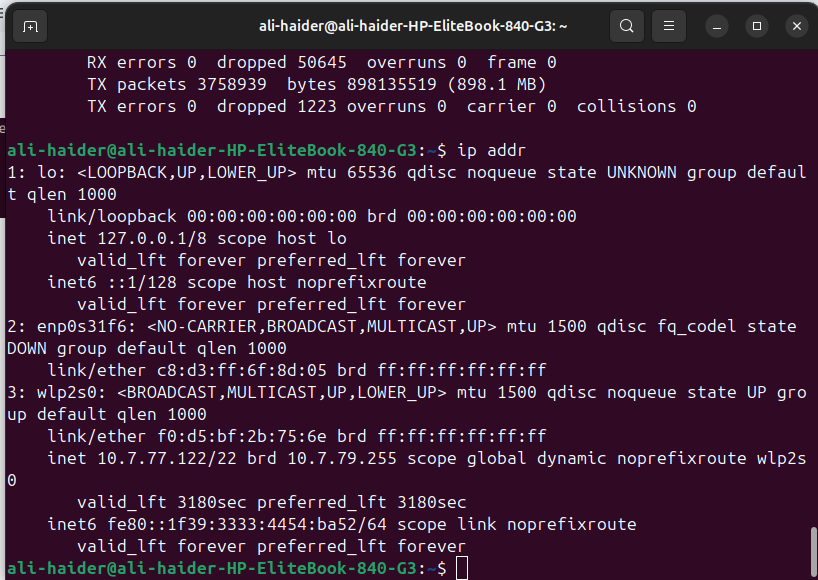
**Commands:**

ifconfig

ip addr

**Explanation:** Displays active network interfaces and IP configuration.

**Output:**



### **Task 2.5 – DNS Lookup**

**Commands:**

nslookup google.com

dig google.com

**Explanation:** Queries DNS to resolve domain names to IPs.

**Output:**



### **Task 2.6 – Download Test File**

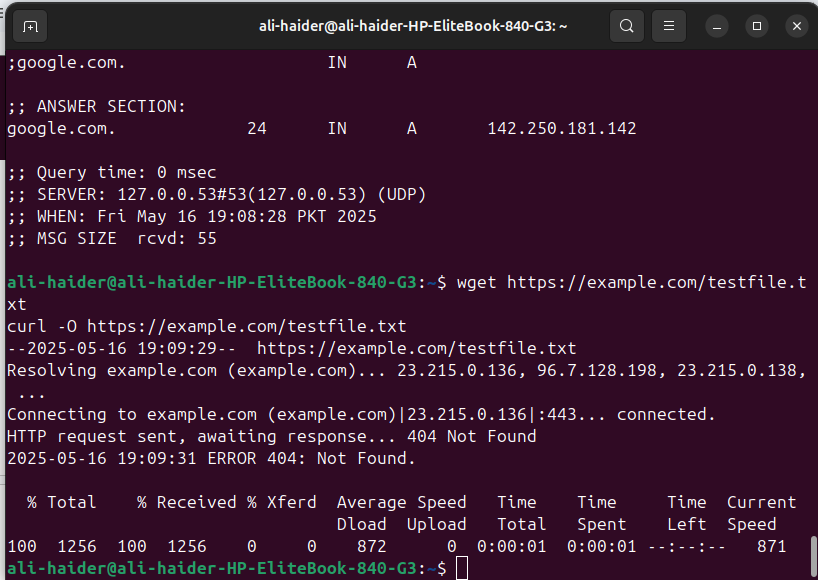
**Commands:**

wget https://example.com/testfile.txt

curl -O https://example.com/testfile.txt

**Explanation:** Fetches a file from the internet using wget and curl.

**Output:**



### **Task 2.7 – Monitor Bandwidth in Real-Time**

**Commands:**

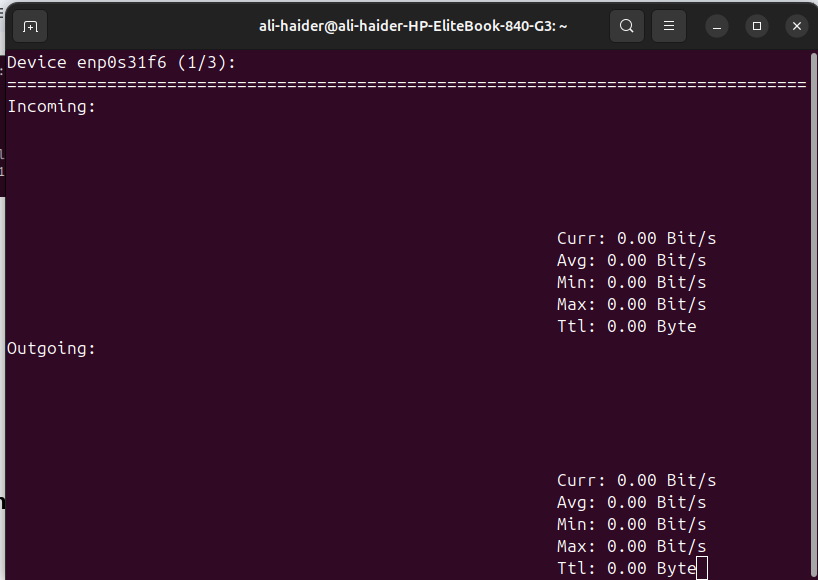
sudo apt install iftop nload

sudo iftop -i eth0

sudo nload eth0

**Explanation:** Monitors real-time bandwidth usage.

**Output:**



## **Part 3: Compression & Decompression**

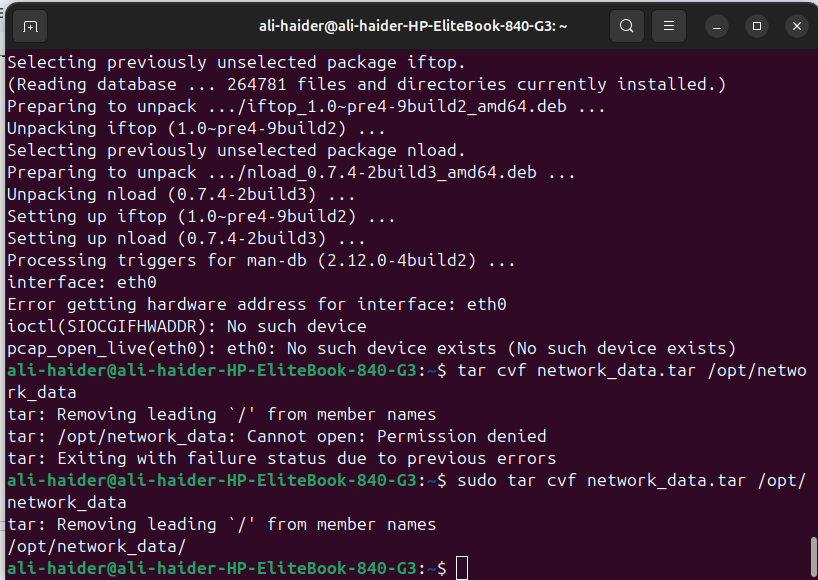
### **Task 3.1 – Archive Directory**

**Command:**

tar cvf network\_data.tar /opt/network\_data

**Explanation:** Creates an uncompressed archive of the shared directory.

**Output:**



### **Task 3.2 – Compress Archive with gzip**

**Command:**

gzip network\_data.tar

**Explanation:** Compresses the archive using gzip.

**Output:**

### **Task 3.3 – Decompress Archive**

**Command:**

gunzip network\_data.tar.gz

**Explanation:** Decompresses the gzip archive.

**Output:**

### **Task 3.4 – Use bzip2 Compression**

**Commands:**

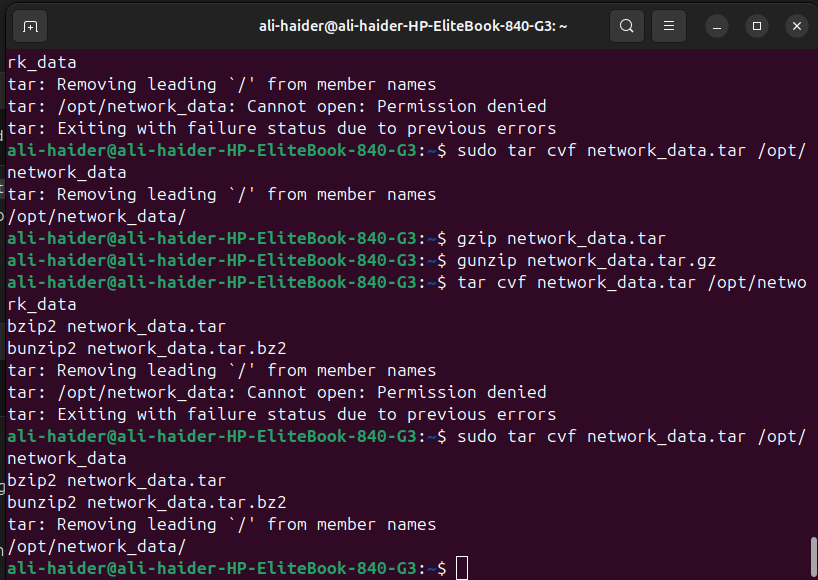
tar cvf network\_data.tar /opt/network\_data

bzip2 network\_data.tar

bunzip2 network\_data.tar.bz2

**Explanation:** Compresses and decompresses using bzip2.

**Output:**

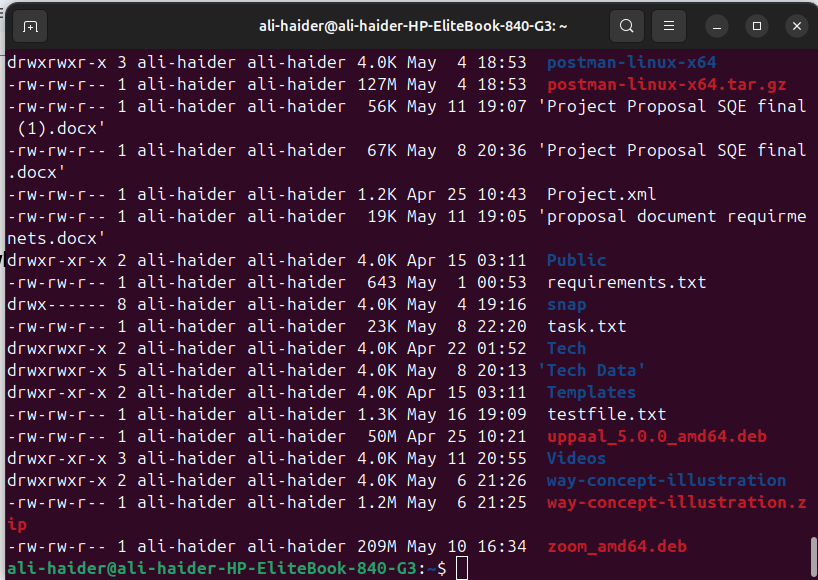


### **File Size Check**

**Command:**

ls -lh

**Output:**



## **Part 4: Text Processing with grep & awk**

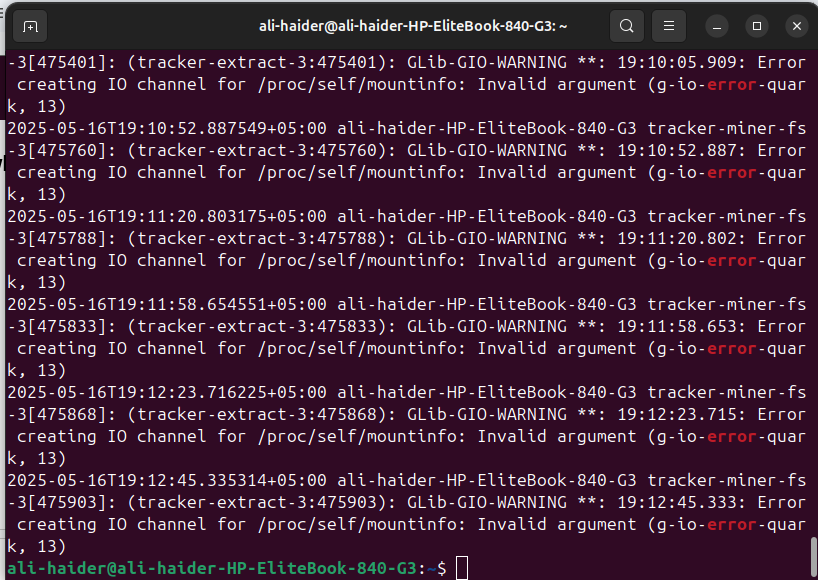
### **Task 4.1 – Search for "error" in Log Files**

**Command:**

grep "error" /var/log/syslog

**Explanation:** Searches for error entries in the system log.

**Output:**



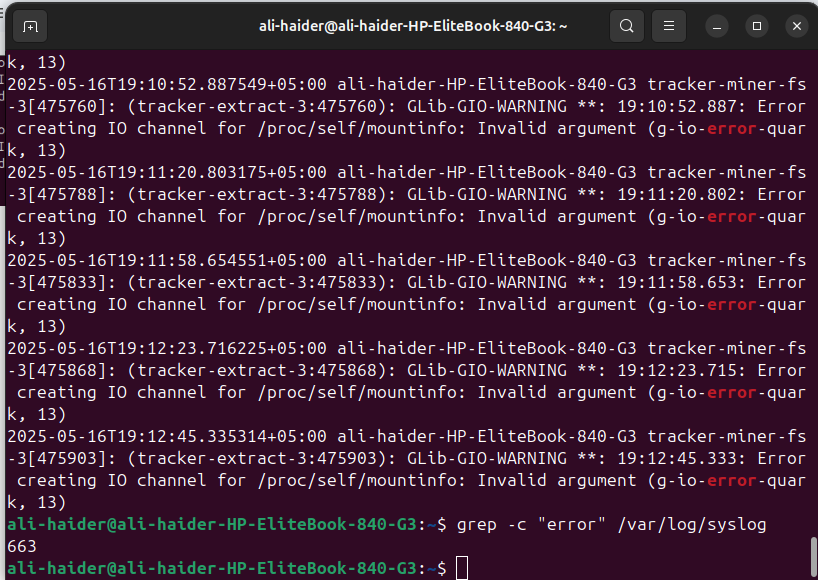
### **Task 4.2 – Count How Many Errors Found**

**Command:**

grep -c "error" /var/log/syslog

**Explanation:** Counts occurrences of the word "error".

**Output:**



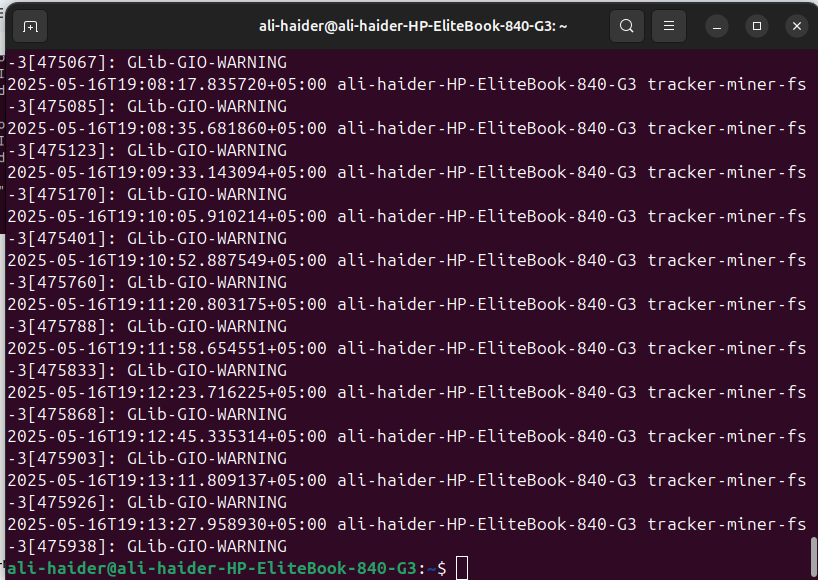
### **Task 4.3 – Extract Specific Fields**

**Command:**

grep "error" /var/log/syslog | awk '{print $1, $2, $3, $5}'

**Explanation:** Extracts timestamp and source from log entries.

**Output:**



### **Task 4.4 – Combine Commands to Summarize**

**Command:**

grep "error" /var/log/syslog | awk '{print $5}' | sort | uniq -c | sort -nr

**Explanation:** Counts and sorts error sources to summarize logs.

**Output:**

