DFCL Lab Assignment - LAB 1
Objective: To explore various Linux commands that will be useful in forensic investigation.

Instructions:

1. Provide the complete commands for all the exercises where asked for the command, and provide a descriptive answer where asked for an explanation. There may be multiple answers/commands for these exercises, so feel free to submit the answer you feel most comfortable with.
2. Organize the files in a folder named using your **roll number** (e.g., RollNo_12345).
3. Compress (zip) the folder.
4. Upload the zipped folder to the **LAB 1 Student Assignment** folder provided on Microsoft Teams.

Deliverables:

- A zipped folder containing the files, named with your roll number.

Submission Deadline:
[20-01-2025]

Lab Questions:

1. If we wanted to list all the .txt files in the current directory, what command would we want to use?

2. What command can we use to read the contents of the file /etc/passwd?

3. If we wanted to search for the string Error in all files in the /var/log directory, what would our command be?

4. What would be the commands to calculate MD5 and SHA1 hashes of the file /etc/passwd?

5. Use the file command to determine the type of the file /usr/bin/cat and explain the output in 2-3 sentences.

6. What command can we use to display all printable strings of length ≥ 8 in the file /bin/bash?

7. Given the following output of the file command, can you determine what's wrong with this file?

$ file image.jpg

image.jpg: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=3ab23bf566f9a955769e5096dd98093eca750431, for GNU/Linux 3.2.0, not stripped

8. If we wanted to look for files modified in the last 30 minutes in /home directory, what command would we want to use?

Hint: Explore how you can use find command to achieve this.

9. What command can we use to display information about all active TCP connections on the system?

10. Given 3 corrupted image file, can you find a way to recover and view its contents?

Hint 1: A quick google search for “magic bytes” might help.

Hint 2: Explore how hexedit can help you here. The three corrupted files are named one, two and Three.