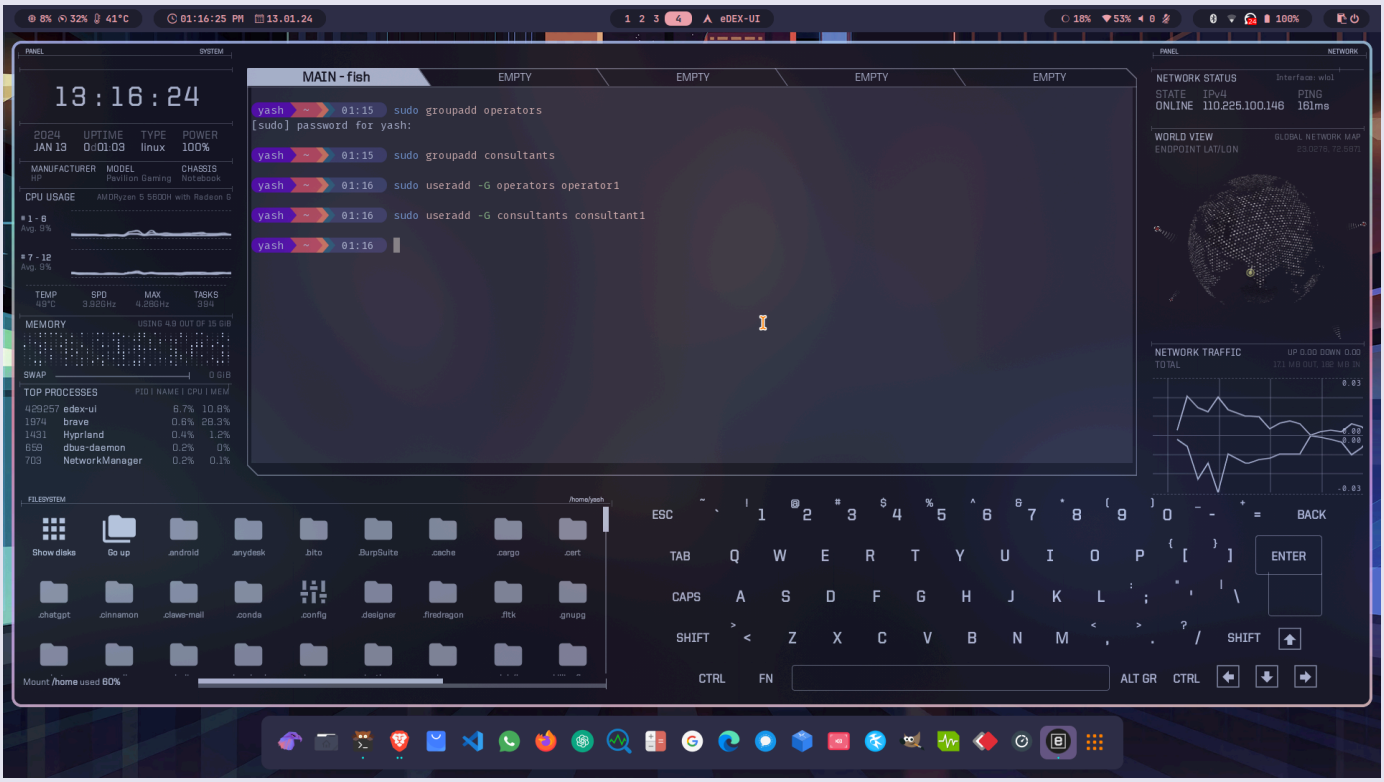
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

Exercises :

1. **Operators and Consultants are members of an IT support company. They need to start sharing information. servera contains a properly configured share directory located at /shares/content that hosts files. Currently, only members of the operators group have access to this directory, but members of the consultants group need full access to this directory. The consultant1 user is a member of the consultants group but has caused problems on many occasions, so this user should not have access to the directory. Your task is to add appropriate ACL entries to the directory and its contents so that members of the consultants group have full access, but deny the consultant1 user any access. Make sure that future files and directories stored in /shares/content get appropriate ACL entries applied.**

Steps and Screenshots :

a) Creating users and groups required.



Command : **sudo groupadd <groupname>**

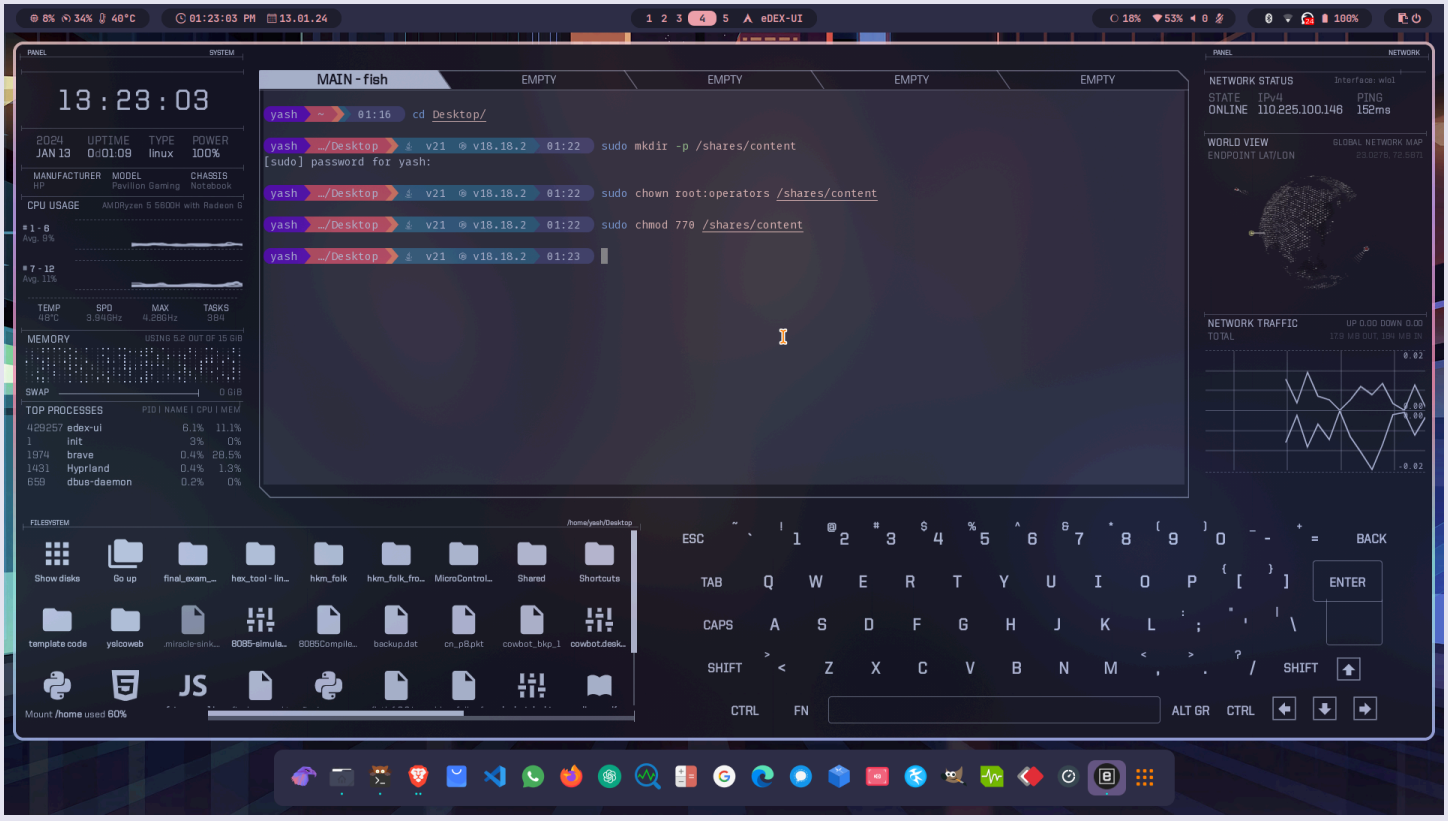
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

Explanation : ***sudo*** for root privileges, ***groupadd*** for creating a user group with name specified

Command : **sudo useradd -G <groupname> <username>**

Explanation : ***sudo*** for root privileges, ***useradd*** for creating user if not exists, ***-G*** for supplementary group specification, either name or groupID specified and then group's and user's name. It creates a new user with name specified adding it to supplementary group of name specified.

b) Creating required folders with necessary permissions.



Command : **sudo mkdir -p /shares/content**

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

Explanation : ***sudo*** for root privileges, ***mkdir*** for creating directory, ***-p*** for creating parent directory also if not exists and then the directory name

Command : **sudo chown root:operators /shares/content**

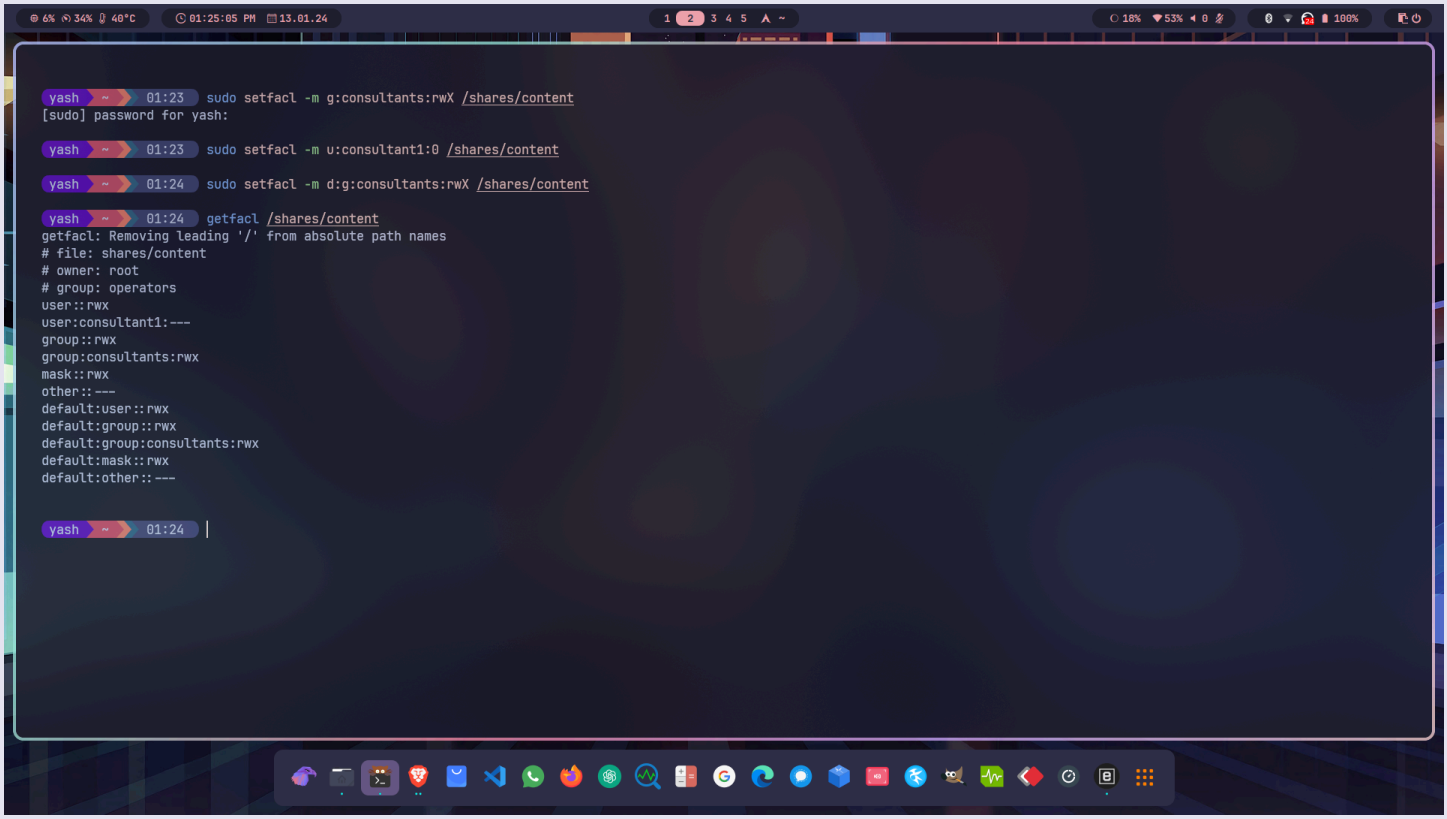
Explanation : ***chown*** for changing ownership of the directory specified to ***user:group*** format specified and empty if not required like ***chown user: <dir>*** or ***chown :group <dir>***

Command : **sudo chmod 770 /shares/content**

Explanation : ***chmod*** for changing the permissions of the directory and its contents or a file specified, ***770*** is specified with format ABC, where A digit is for user permissions, B for its group and C for others. Permission digits are : 4 for read, 2 for write, 1 for execute and their summation for combinations. Here 7 means all rwx permissions.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

c) Setting file permissions via setfacl command



Command : **sudo setfacl -m g:consultants:rwX /shares/content**

Explanation : ***setfacl*** is used to manipulate the ACL (Access Control List) of a file or a directory, ***-m*** for modifying the ACL directly from the command (otherwise -M for modifying ACL of a file from another file where ACL entries are written), ***g:consultants:rwX*** for permitting group named consultants, the rights to read, write and execute. Here, ***X*** is used because, it checks the condition first if any user or group has execute rights, if yes, then allows x permission, otherwise it has no effect. The name of directory here specified is ***/shares/content.*** A file name also can be used.

Command : **sudo setfacl -m u:consultant1:0 /shares/content**

Explanation : Here, similar to previous command, but, ***u:consultant1:0*** means, for ***user*** named ***consultant1***, ***0*** means no rights are permitted for the directory specified.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

Command : **sudo setfacl -m d:g:consultants:rwX /shares/content**

Explanation : This is similar to the first command for group access. The difference here is ***d:*** used, which means the access is modified also for subdirectories and subfiles of the directory specified. Alternatively, here ***-d*** can be used with setfacl along with g:groupname:rights.

Command : **getfacl /shares/content**

Explanation : ***getfacl*** is used to get the ACL of a directory or a file specified. It gives stdout output text with ACL entries of ***/shares/content.***

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

2. **Create a txt file in a folder and allow only a specific user the read and execute access. Ensure that the user is not able to modify the content of the file.**

Command : **touch itim-p2/demo.txt**

Explanation : ***touch*** is used to create an empty plain text file. The file created is ***demo.txt*** inside the ***itim-p2*** folder.

Command : **echo “Demo file” > itim-p2/demo.txt**

Explanation : ***echo*** is used to print the text or a variable specified to stdout. Here, “***Demo file”*** text is given to stdout, which is redirected as stdin for ***demo.txt*** file inside ***itim-p2*** folder using ***‘>’.*** Hence, text specified here will be printed to the specified file.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

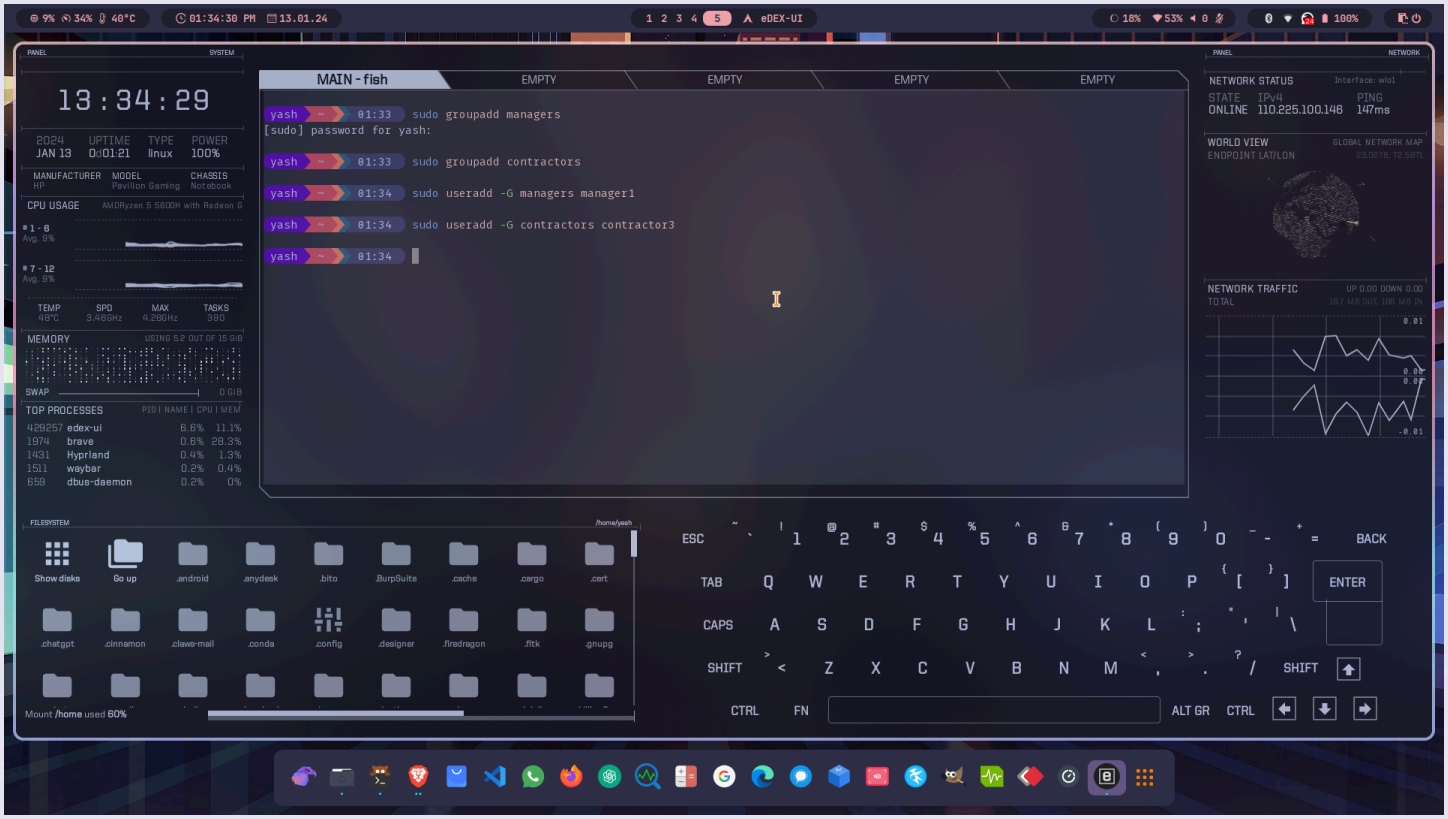
Command : **sudo setfacl -m u:yash:rx demo.txt**

Explanation : Similar to previous commands, here, ***u:yash:rx*** indicates that the read and execute permissions are given to the ***user*** named ***yash*** for the file ***demo.txt.*** Here, ***x*** is used to give execute permission simply anyhow, unlike ***X,*** which first checks the condition.

3. **A stock finance agency is setting up a collaborative share directory to hold case files, which members of the managers group will have read and write permissions on. The co-founder of the agency, manager1, has decided that members of the contractors group should also be able to read and write to the share directory. However, manager1 does not trust the contractor3 user (a member of the contractors group), and as such, contractor3 should have access to the directory restricted to read-only. manager1 has created the users and groups, and has started the process of setting up the share directory, copying in some templates files. Because manager1 has been too busy, it falls to you to finish the job. Your task is to complete the setup of the share directory. The directory and all of its contents should be owned by the managers group, with the files updated to read and write for the owner and group (managers). Other users should have no permissions. You also need to provide read and write permissions for the contractors group, with the exception of contractor3, who only gets read permissions. Make sure your setup applies to existing and future files.**

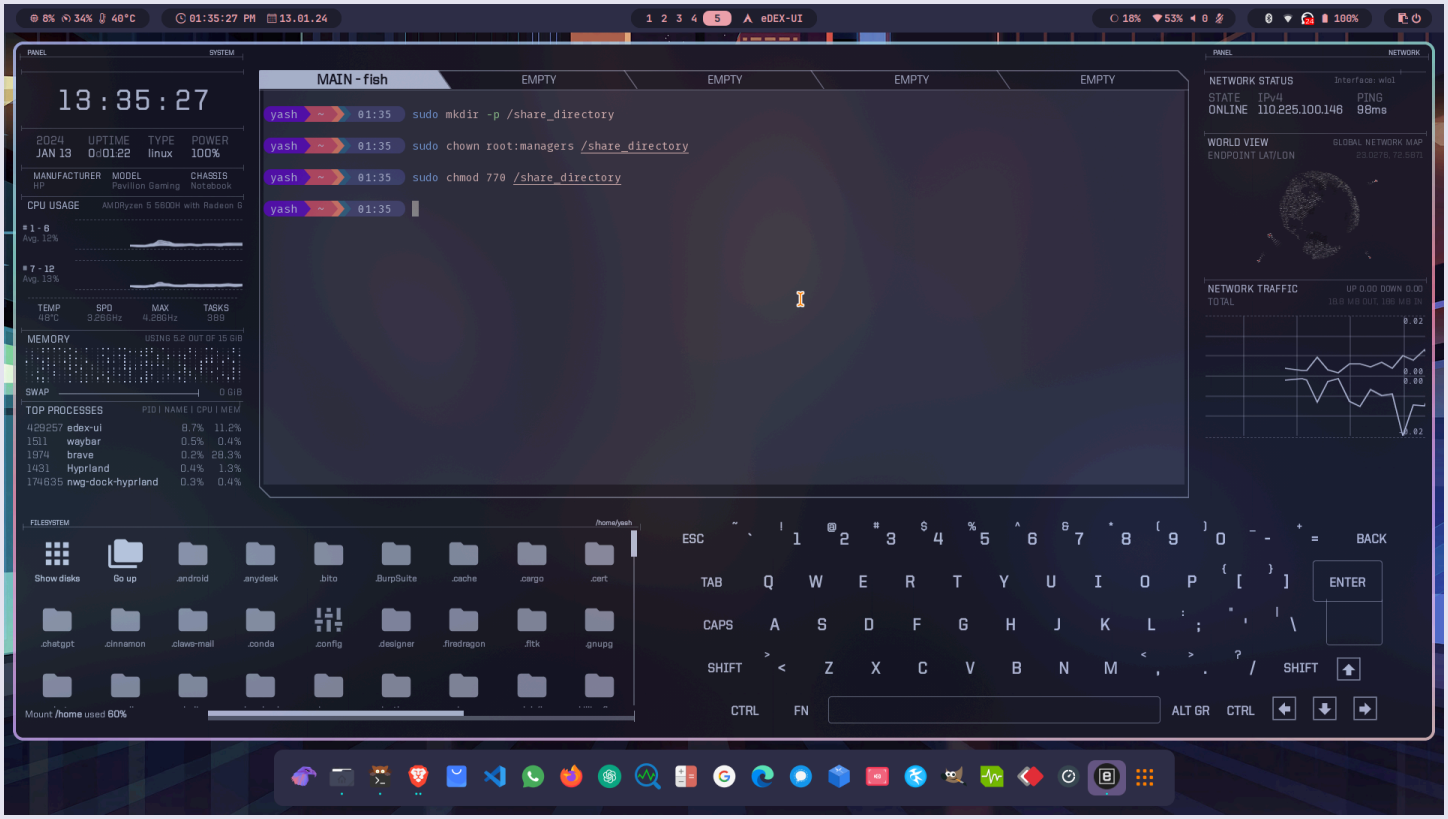
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

a) Creating users and groups required.



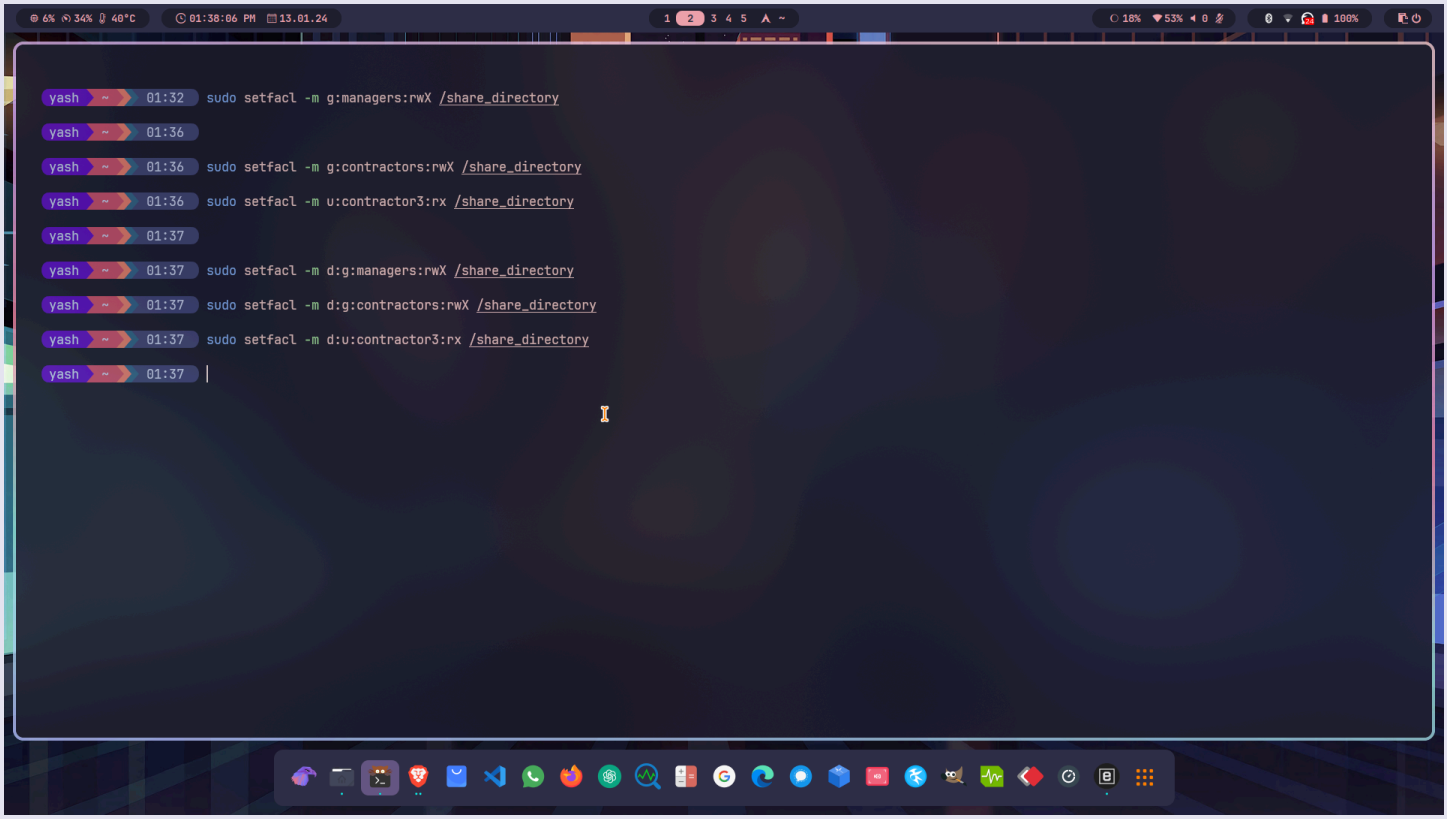
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

b) Creating directory required with necessary permissions.



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

c) Setting and modifying permissions via ACL.



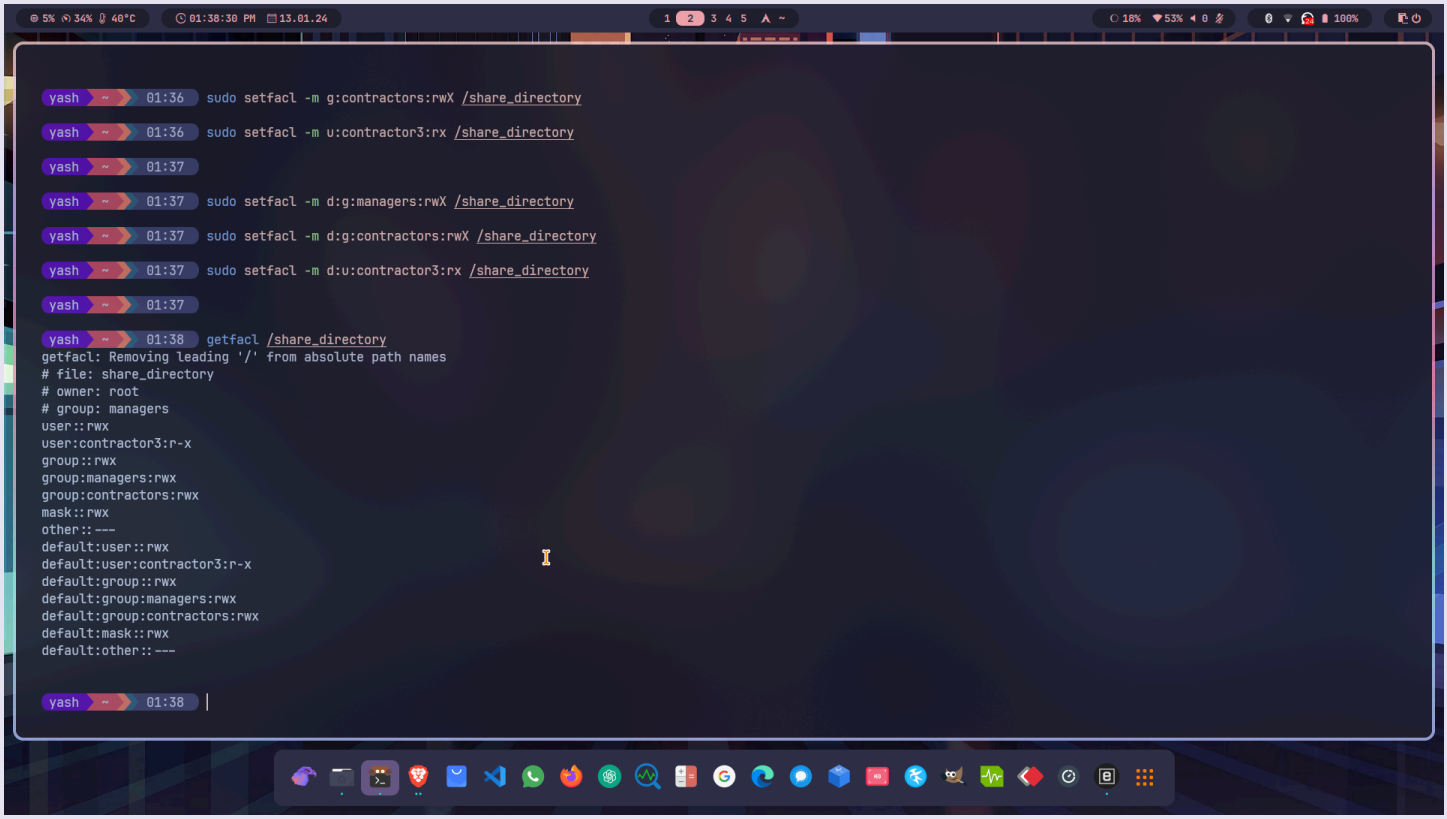
Commands :

- **sudo setfacl -m g:managers:rwX /share_directory**
- **sudo setfacl -m g:contractors:rwX /share_directory**
- **sudo setfacl -m u:contractor3:rx /share_directory**
- **sudo setfacl -m d:g:managers:rwX /share_directory**
- **sudo setfacl -m d:g:contractors:rwX /share_directory**
- **sudo setfacl -m d:u:contractor3:rx /share_directory**

Explanation : Same as previous commands for user, group access and ***x*** and ***X*** for direct and conditioned execute permissions respectively similar to previously used.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
ITIM Practical 2

d) Checking the permissions via ACL entries.



Command : **getfacl /share_directory**