Project code: <https://github.com/Eliran-b/auditd-logs-analysis>

**Main Flow**

The program has 2 main componants raw logs handler and parsed log handler



**find specific audit\_rule logs(by rule\_name index)**



**query the amount of ule\_name and command type in the table**



**The command that appears most frequently**



**The user who executes the most commands**



**The least common command**



**The folder path that has the most activity**



**The number of new entries added to the database between various code runs**

