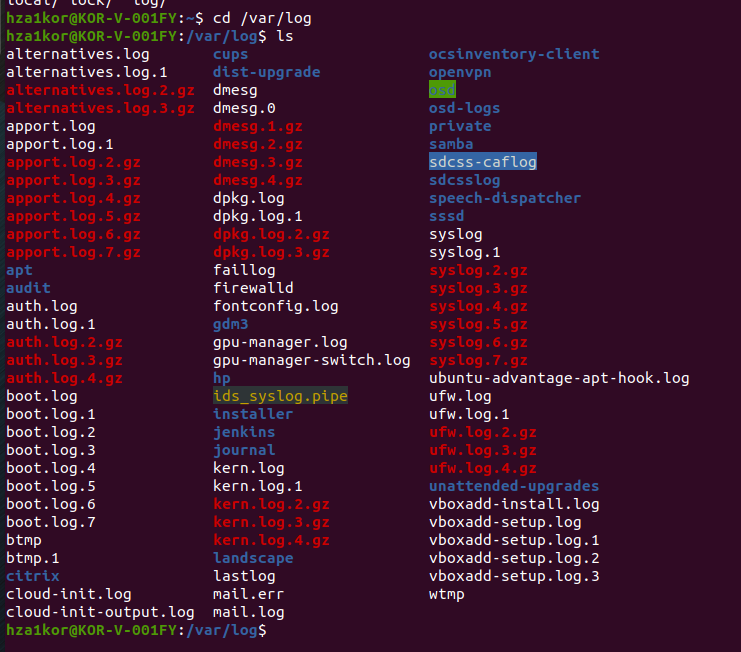
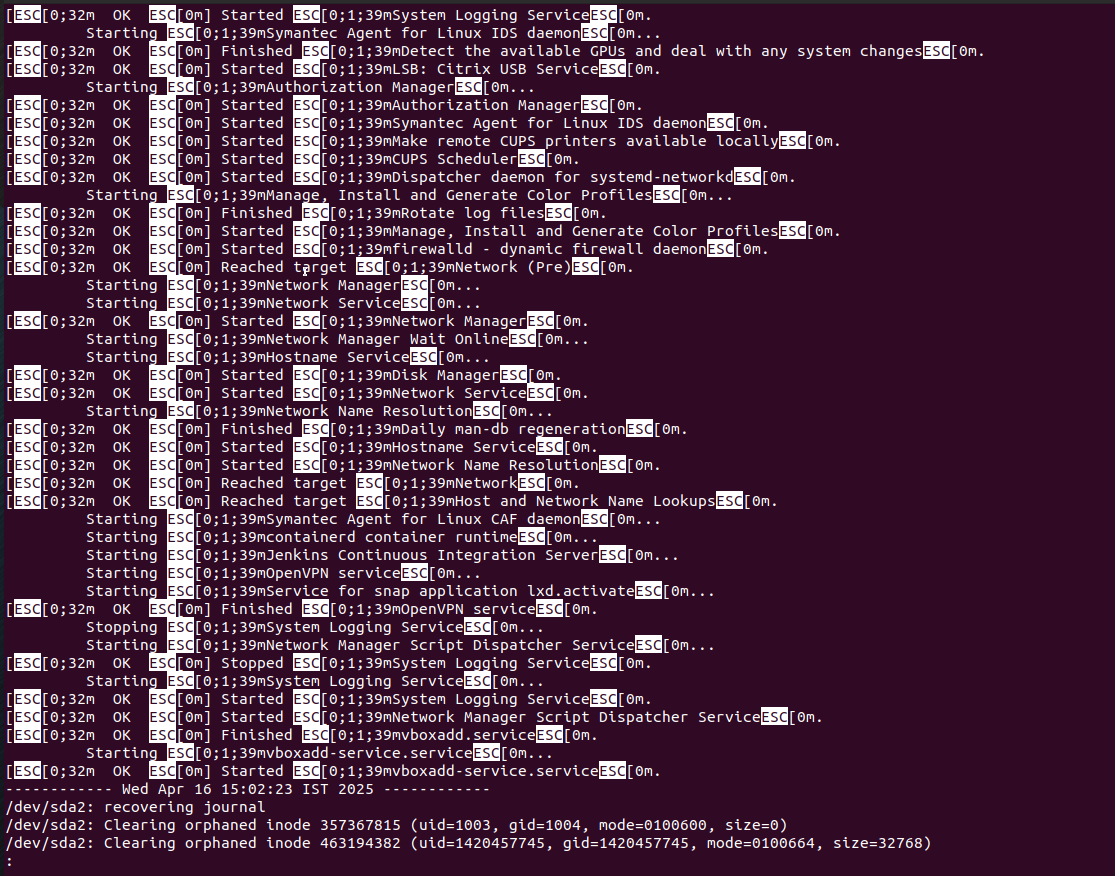
**Linux Log Monitoring | How to Do Log Analysis? | MPrashant**

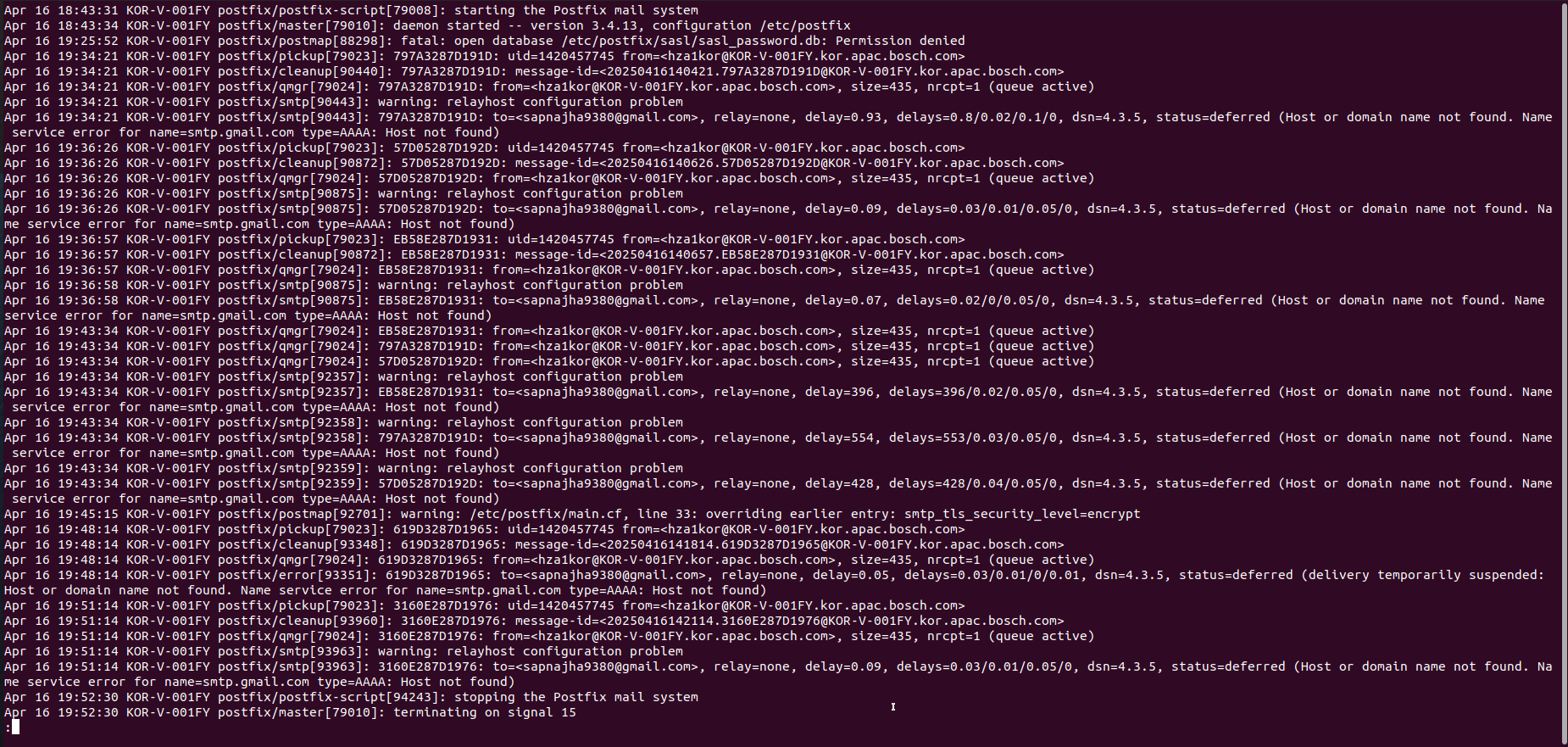
* A log file stores events, processes, messages, and other data from applications, operating systems or devices
* They provide information based on the actions performaed by users, playling an important role in monitoring
* All the linux logs are saved in /var/log



* The important log files to look at
  + boot – logs related to system startup



* + chron – logs related to chron jobs(automated jobs)
  + secure – logs related to login activities, authentication failures
  + maillog - logs related to mailing services like sendmail or mailx



* + httpd – logs related to web server
  + messages – all logs related to the linux server
* say I want to find if there are any errors in the file – grep -I “error” filename
* say I want to find any warning in a file – grep -i “error” <filename>
* say I want to search for error and warning in a file – egrep -i “error|warning” <filename>
* say I want to check how many times error came – cat <filename> | grep -i “error” | wc -l