Objective

The next tasks are all about dealing with log files and working out the format of the file, extracting data and presenting it. For each of the tasks we want you to document the commands used and your output.

The ExampleFinance.log file can be found in /home/shared — copy that file into your own home directory and do the tasks using the copied file

Task 1

In this task we want you to view the data in the log file in different ways so that you get to understand the format of the log file. Once you think you have the format of the logfile write out the syntax for it.

1. View the ExampleFinance.log file page by page, making note of the lines and working out what the format of the line is. You should look for the default field separator and whether the log file has multiple lines for a message, or whether each line is a unique message
2. Check that you have identified the correct field separator by using a command to count the number of lines that contain your field separator
3. Check that there are not any lines that do not contain the field separator
4. How many lines are there in the file in total?
5. Write down your idea of what each column of the log file is called;

Task 2

Now that you have worked out the format of the data we would like you to provide a summary of the following. In your work you should tell us;

- The command you ran
- The result of the command

1. Tell me how many of each type of message there are in the log file and sort them biggest first;
2. Tell me the top 5 times with the highest number of messages in the log file that occurred at the same time on specific days, with the highest being printed first.
3. Using your command in 2, change it so that you get the bottom 5
4. Using your commands in 2 and 3, write the outputs so that they are both in a file called topbottomtimes.txt

Task 3

Data separation. In this task we want you to separate out data into separate files.

- Separate out each type of message into its own file.
  - e.g. all lines with errors into a file called errors.log, all lines with info into a file called info.log, etc
- Let's check to make sure that we only have errors for error messages. Construct a command that will check this for us, and provide us with a short summary output, e.g. tells us how many of each message.
- Check the other files too
- How many lines are there in each of the files? Do this in one command line

Task 4

Earlier we asked you to look for those lines that contained the extra field separators which were financial trading information.

- Is there a correlation between the lines in the log file that contain the word **time=** and the type of **notice**?
- What are the 3 eventTypes in the log file?