Name: Mosab Fathy Ramadan Mohamed
Group: B20-SD-01
Lab 4: Text filtering editors

Save the following lines to a file `server-data.log` .

```
25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24'
25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24'
25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
3 13:25:35 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24'
25:35 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24' END
25:35 wazuh-remoted: ACTION: none INFO: Remote syslog allowed from: '10.110.15.0/24'
```

> The following tasks are to be completed with either grep, sed, or awk.
> All actions are to be performed on `server-data.log`

```
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ ls
server-data.log
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ cat server-data.log
2022/09/18 13:25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
Log1 2022/09/18 13:25:35 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:35 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24' END
2022/09/18 13:25:35 wazuh-remoted: ACTION: none INFO: Remote syslog allowed from: '10.110.15.0/24'
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$
```

1. View only error and warning messages in `server-data.log`. Show how you can do this with grep and awk.

Answer:

grep:

"$ grep -P '(ERROR|WARNING)' server-data.log"

```
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ grep -P '(ERROR|WARNING)' server-data.log
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$
```

awk:

"$ awk '/ERROR|WARNING/{print}' server-data.log"

```
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ awk '/ERROR|WARNING/{print}' server-data.log
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$
```

2. View every line except lines with informational messages.

Answer:

"$ sed '/INFO/ d' server-data.log"

```
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ sed '/INFO/ d' server-data.log
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$
```

3. Count how many error messages are in the log.

Answer:

"$ grep -c ERROR server-data.log"

```
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ grep -c ERROR server-data.log
2
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$
```

4. Replace all mentions of "INFO" with "NOTHING" and save the output to a file `newlog.log`.

Answer:

"$ sed 's/INFO/NOTHING/g' server-data.log > newlog.log"

```
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ sed 's/INFO/NOTHING/g' server-data.log > newlog.l
og
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ cat newlog.log
2022/09/18 13:25:34 wazuh-remoted: NOTHING: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:34 wazuh-remoted: NOTHING: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
Log1 2022/09/18 13:25:35 wazuh-remoted: NOTHING: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:35 wazuh-remoted: NOTHING: Remote syslog allowed from: '10.110.15.0/24' END
2022/09/18 13:25:35 wazuh-remoted: ACTION: none NOTHING: Remote syslog allowed from: '10.110.15.0/
24'
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$
```

5. Write a single regular expression to match the following lines in the file. Show the full command and regex used.

```
2022/09/18 13:25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18
2022/09/18 13:25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.1
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18
```

Try to be as strict as possible when matching. Find the common patterns and match them as much as you can.
For example, using the wildcard `.` to match huge portions of the lines reduces the quality of the regex.

> Of course, you can use wildcards. Just don't use them excessively.

Answer:
"$ grep -P "^(((\d+\/){2})\d+)\s((\d+:){2}\d+)\s(\w+-\w+):\s([A-Z]+):(\s[A-Za-z]+)+:\s('((\d+\.)+\d)\/(\d+)')$" server-data.log"

regex:
^(((\d+\/){2})\d+)\s((\d+:){2}\d+)\s(\w+-\w+):\s([A-Z]+):(\s[A-Za-z]+)+:\s('((\d+\.)+\d)\/(\d+)')$
Which consists of 6 parts
1- date: (((\d+\/){2})\d+)
2- time: ((\d+:){2}\d+)
3- wazuh-remoted: (\w+-\w+)
4- log title: ([A-Z]+)
5- log description: ((\s[A-Za-z]+)+)
6- ip: ('((\d+\.)+\d)\/(\d+)')

We also write ^ at the start and $ at the end to specify that this is the whole expression and nothing more or less should be after or before it.

```
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ grep -P "^(((\d+\/){2})\d+)\s((\d+:){2}\d+)\s(\w+
-\w+):\s([A-Z]+):(\s[A-Za-z]+)+:\s('((\d+\.)+\d)\/(\d+)')$" server-data.log
2022/09/18 13:25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$
```

Bonus

6. Consider the following log:

```
at com.databricks.backend.daemon.data.client.DatabricksFileSystemV2.recordOperat
at com.databricks.backend.daemon.data.client.DBFSV2.initialize(DatabricksFileSys
at com.databricks.backend.daemon.data.client.DatabricksFileSystem.initialize(Dat
at org.apache.hadoop.fs.FileSystem.createFileSystem(FileSystem.java:2669)
at org.apache.hadoop.fs.FileSystem.access$200(FileSystem.java:94)
at org.apache.hadoop.fs.FileSystem$Cache.getInternal(FileSystem.java:2703)
```

Write a sed one-liner that will show stack traces lines in the following fashion:

```
Exception occured inside method `org.apache.hadoop.fs.FileSystem$Cache.getIntern

Called method org.apache.hadoop.fs.FileSystem$Cache.getInternal which calls line
```

HINT: sed capture groups are extra useful here

Answer:

“$ sed -nre '6 s/at ([a-zA-Z0-9\.\$]+)\(([a-zA-Z0-9]+\.([a-zA-Z0-9\#]+)):([0-9]+)\)/Exception occured inside method `\1` from file `\2` on line `\4`. The file was written in `\3`/p' bonus.log”

```
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ cat bonus.log
at com.databricks.backend.daemon.data.client.DatabricksFileSystemV2.recordOperation(DatabricksFileS
ystemV2.scala:474)
at com.databricks.backend.daemon.data.client.DBFSV2.initialize(DatabricksFileSystemV2.scala:64)
at com.databricks.backend.daemon.data.client.DatabricksFileSystem.initialize(DatabricksFileSystem.s
cala:222)
at org.apache.hadoop.fs.FileSystem.createFileSystem(FileSystem.java:2669)
at org.apache.hadoop.fs.FileSystem.access$200(FileSystem.java:94)
at org.apache.hadoop.fs.FileSystem$Cache.getInternal(FileSystem.java:2703)
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$ sed -nre '6 s/at ([a-zA-Z0-9\.\$]+)\(([a-zA-Z0-9]+
\.([a-zA-Z0-9\#]+)):([0-9]+)\)/Exception occured inside method `\1` from file `\2` on line `\4`. Th
e file was written in `\3`/p' bonus.log
Exception occured inside method `org.apache.hadoop.fs.FileSystem$Cache.getInternal` from file `File
System.java` on line `2703`. The file was written in `java`
iviosab@iviosab:~/Desktop/GitHub/f22-sna/Week-4$
```