**Lab–Reading Server Logs**

**Part 1: Reading Log Files with Cat, More, and Less**

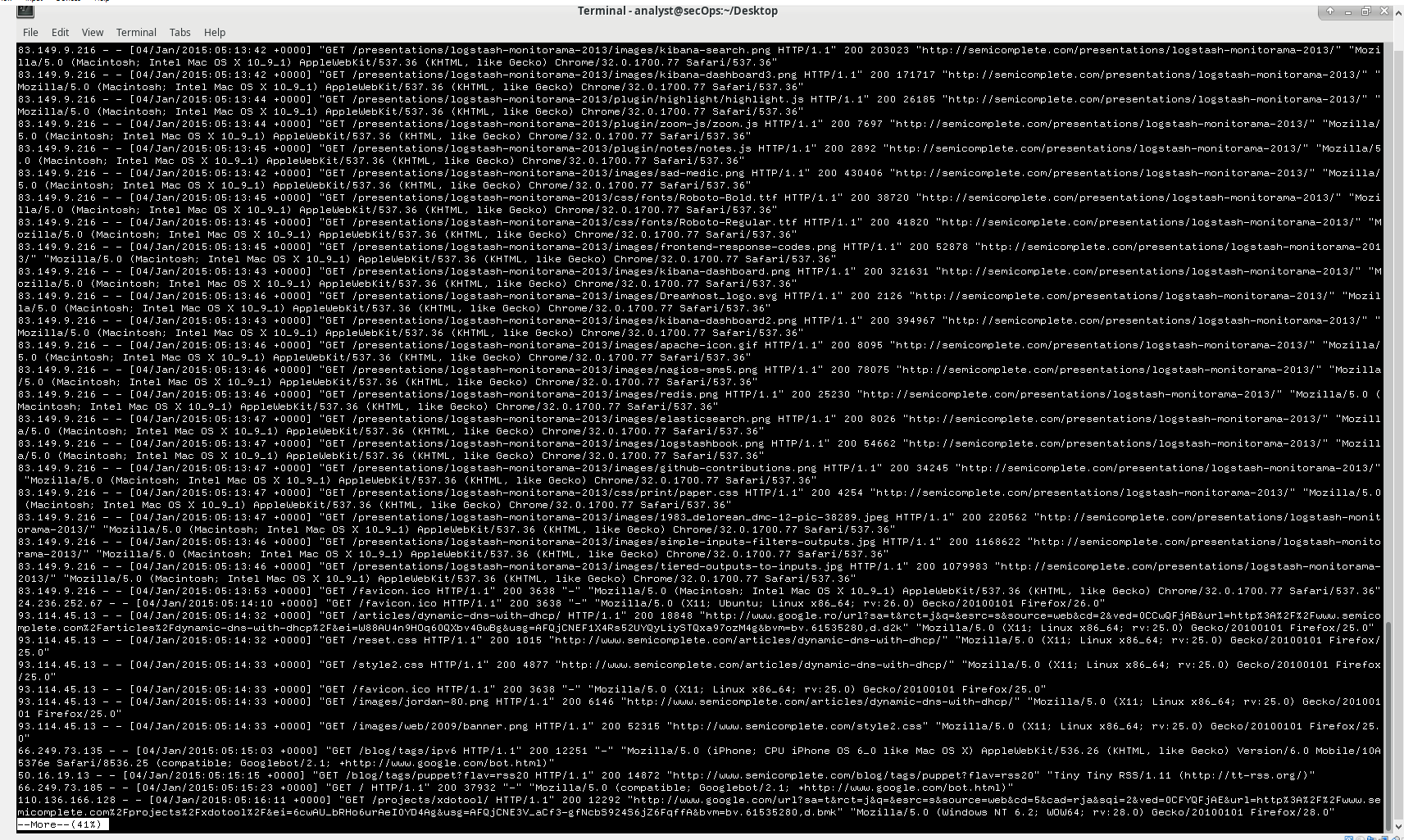
**Step 1:Opening Log Files.**



Cat command usage

**What is a drawback of using cat with large text files?**

Cat has not a page breaking that why beginning of the file can be lost



More command usage

**What is the drawback of using more?**

Command more is slower than less because it loads the entire file at once, but you can navigate by enter



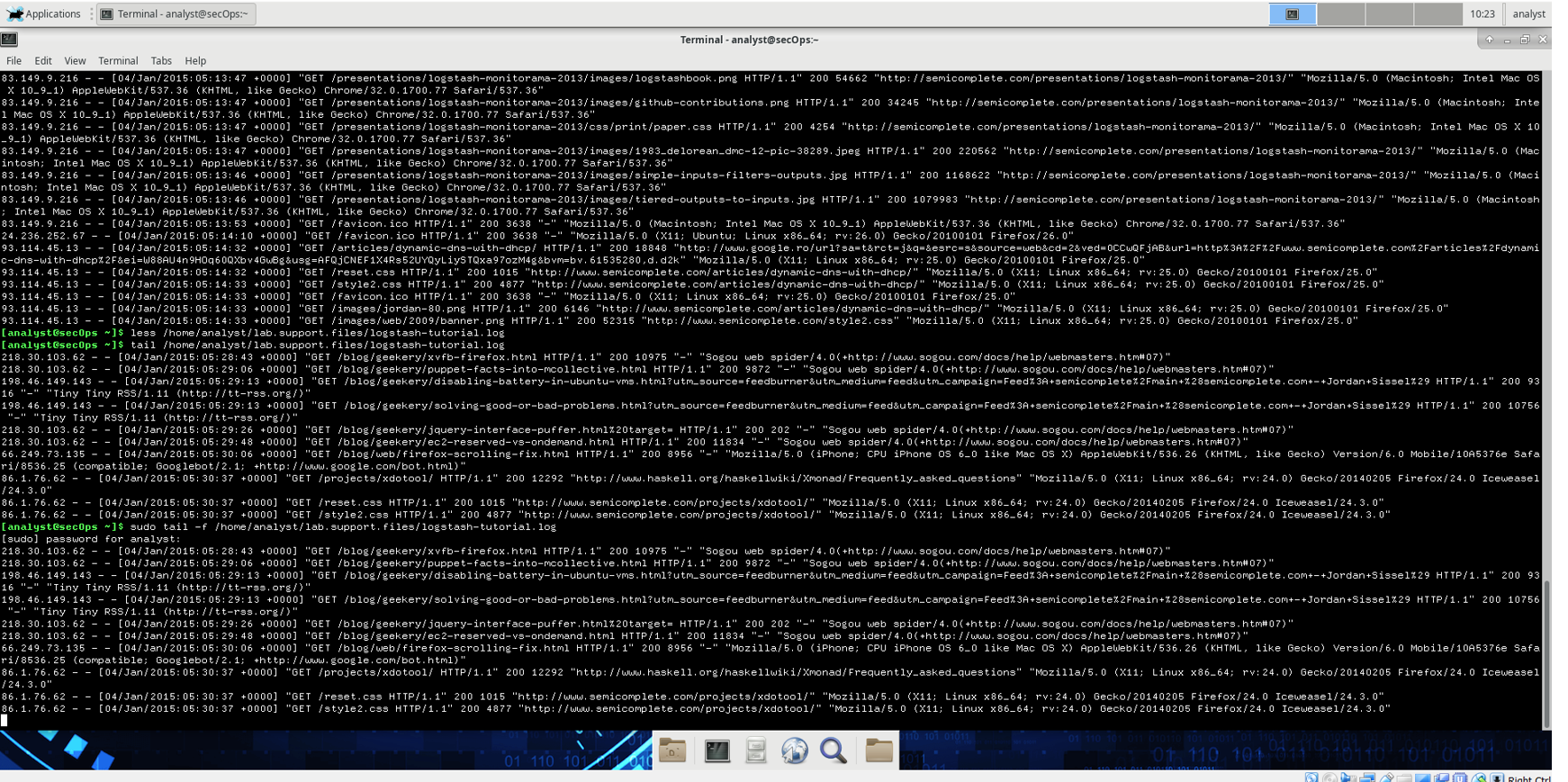
Tail command usage

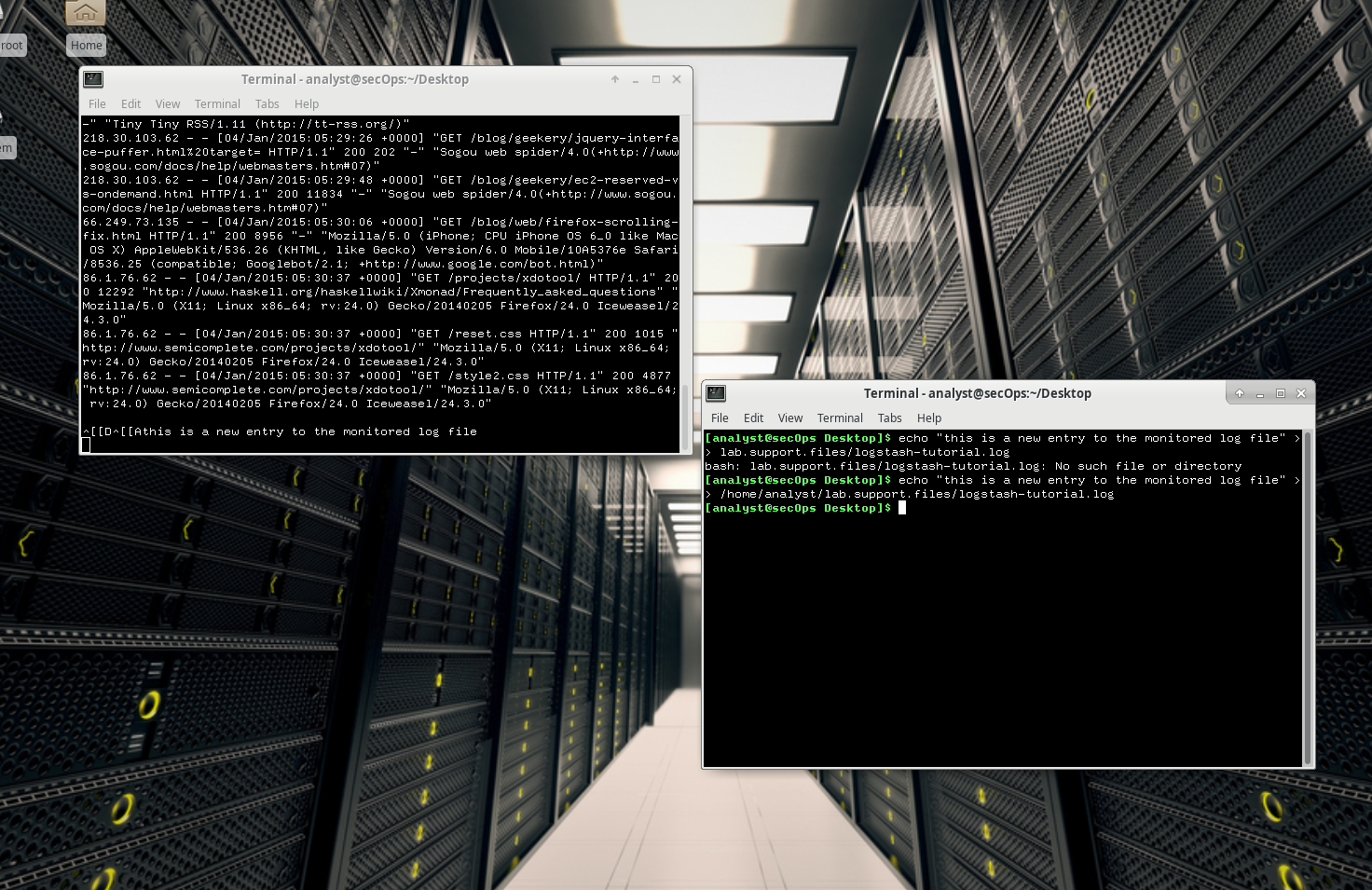


Tail -f command usage

**What is different in the output of tailand tail -f? Explain.**

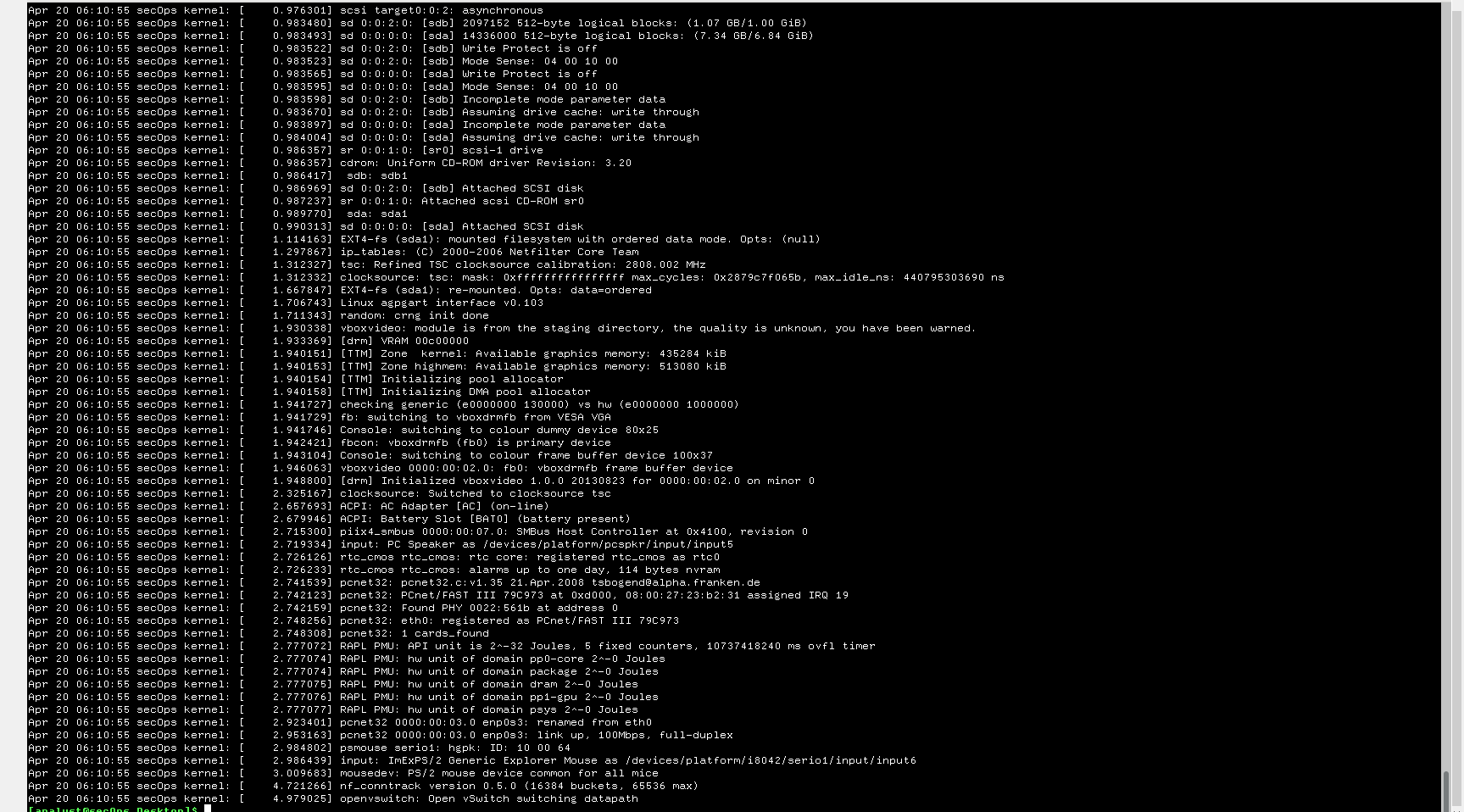
Tail -f command observes in live mode log file while running. That’s why you cannot type any command while running tail -f command





Appending new line in logstash-tutorial.log

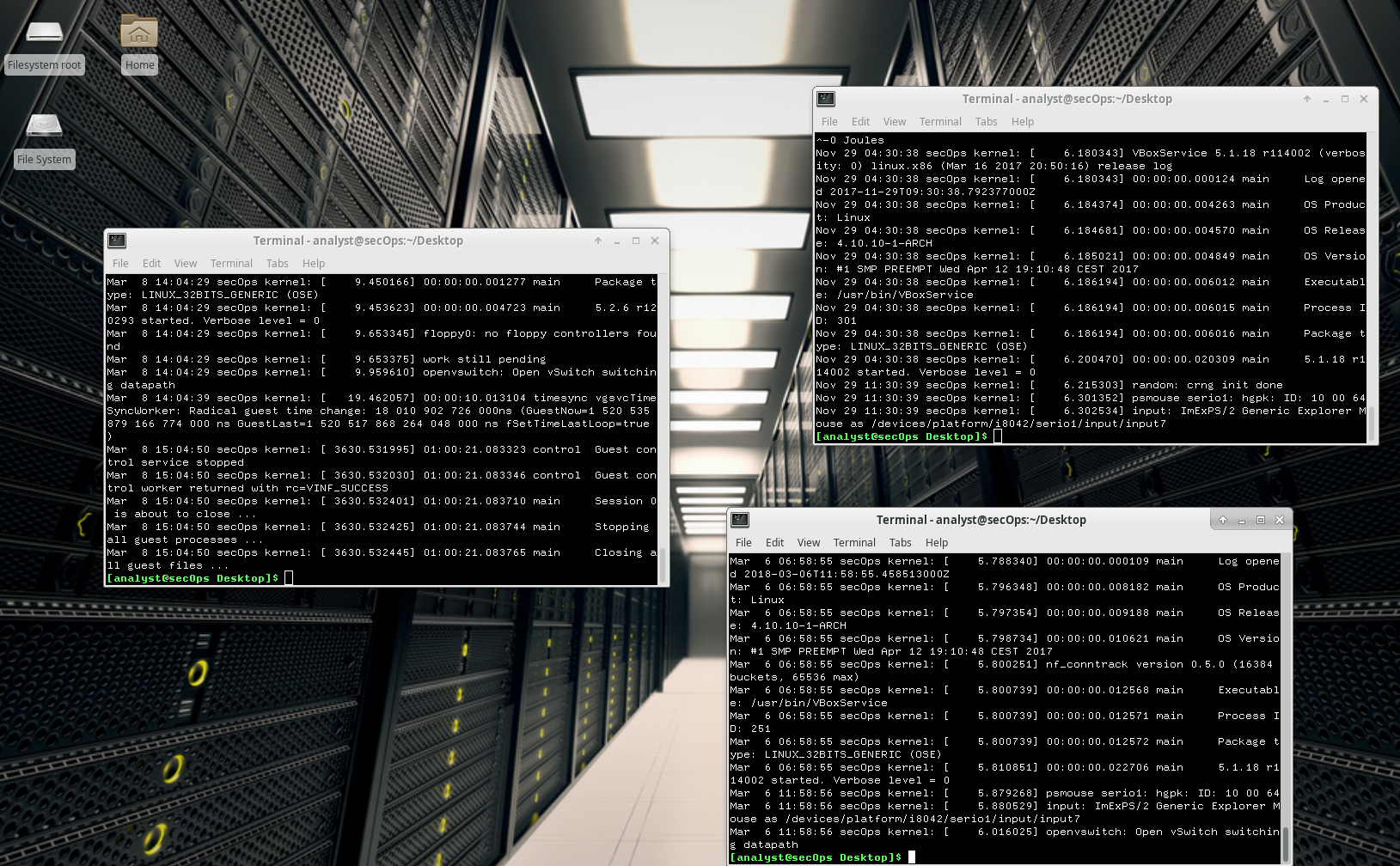
Part 2: Log Files and Syslog



Sudo cat command usage

**Why did the cat command have to be executed as root?**

Because /var/log/syslog.1 lies under the root folder and to access it you should run cat command as a root user

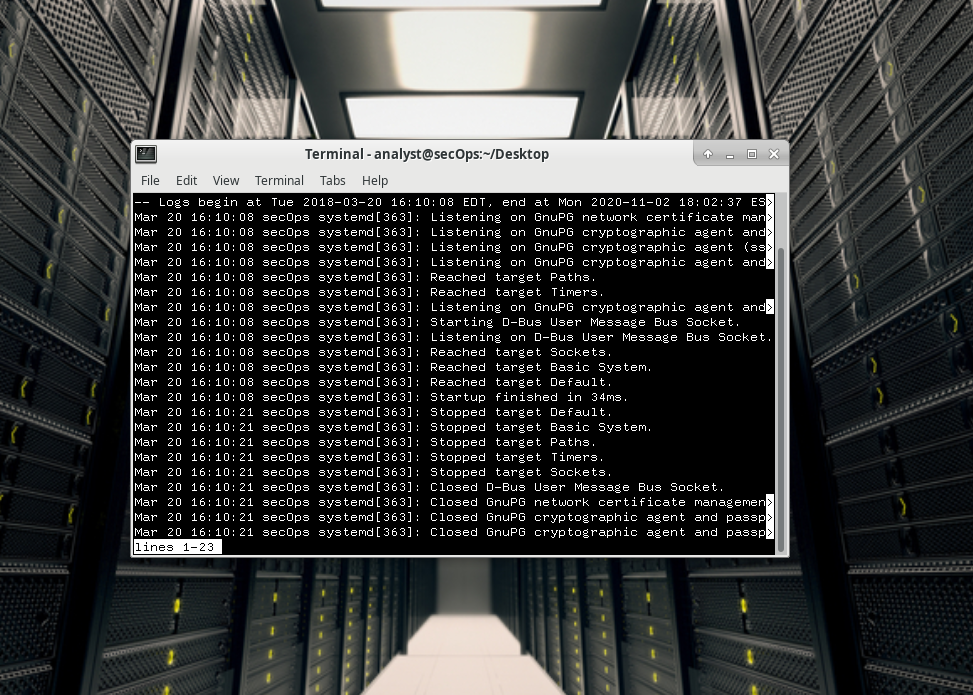


Syslog2,3,4 files

**Can you think of a reason why it is so important to keep the time and date of computers correctly synchronized?**

Date and time is important because it makes easy to make troubleshooting process if something went wrong

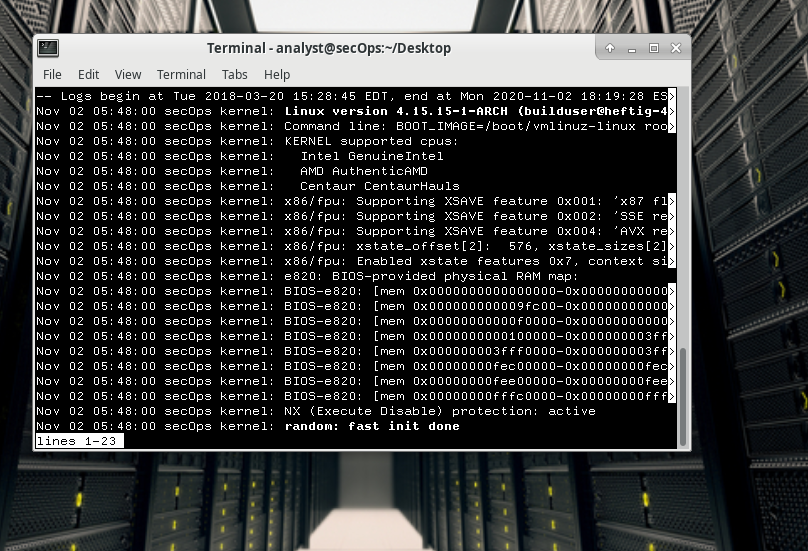
**Part 3: Log Files and Journalctl**



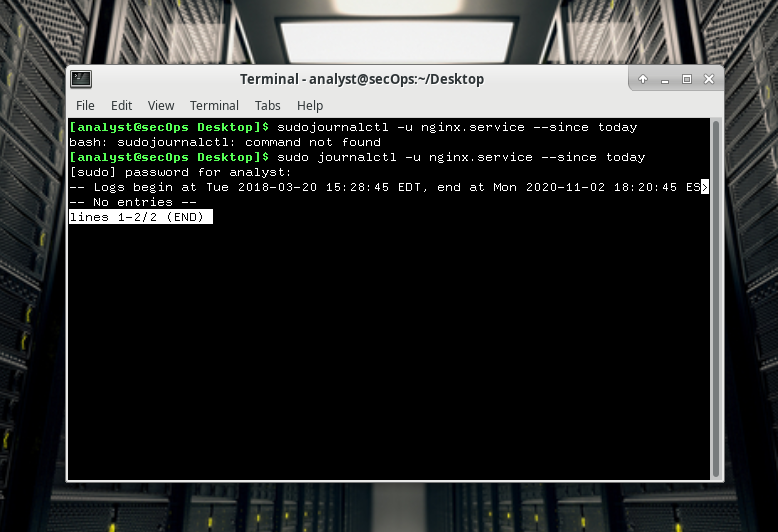
Journalctl command usage



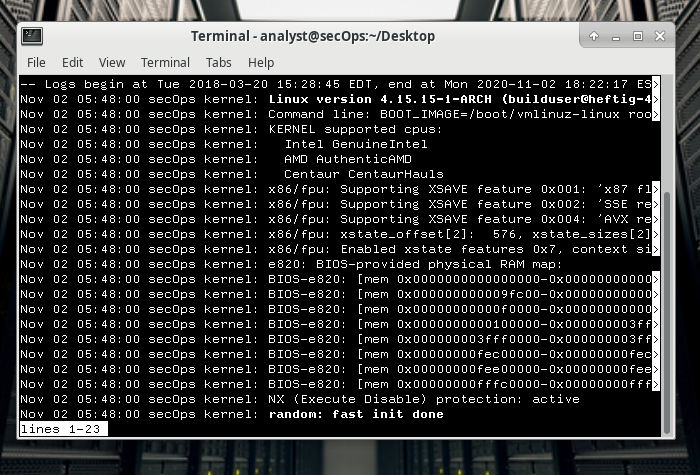
sudo journalctl –utc command usage



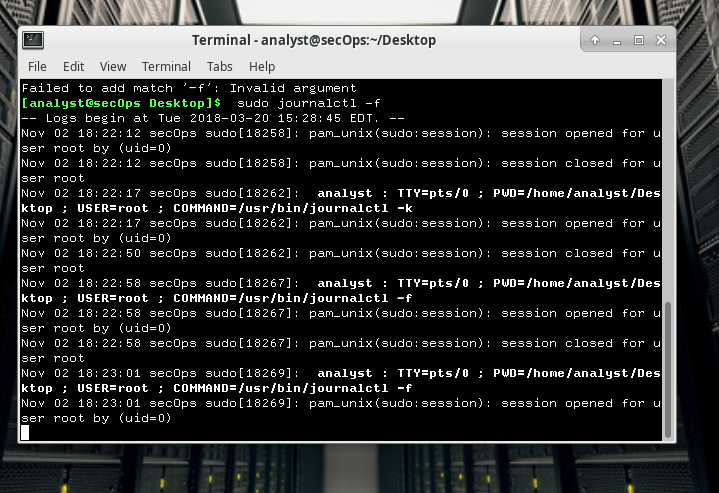
display log entries recorded during the last boot



shows all nginx service logs recorded today



display only messages generated by the kernel



switch to actively follow the logs as they are being written

**Reflection**

**Compare Syslog and Journald. What are the advantages and disadvantages of each?**

System log is a standard logging solution. It uses plain text files, but has no structure. The information is not centralized, and you may need to search through a large amount of unrelated information to find the relevant information. The system log does not allow you to separate messages by related applications. In addition, plain text files may require rotation to prevent them from becoming too large. Journald replaced the log file with plain text in a special file format for log messages. This makes it easier to find relevant log messages.