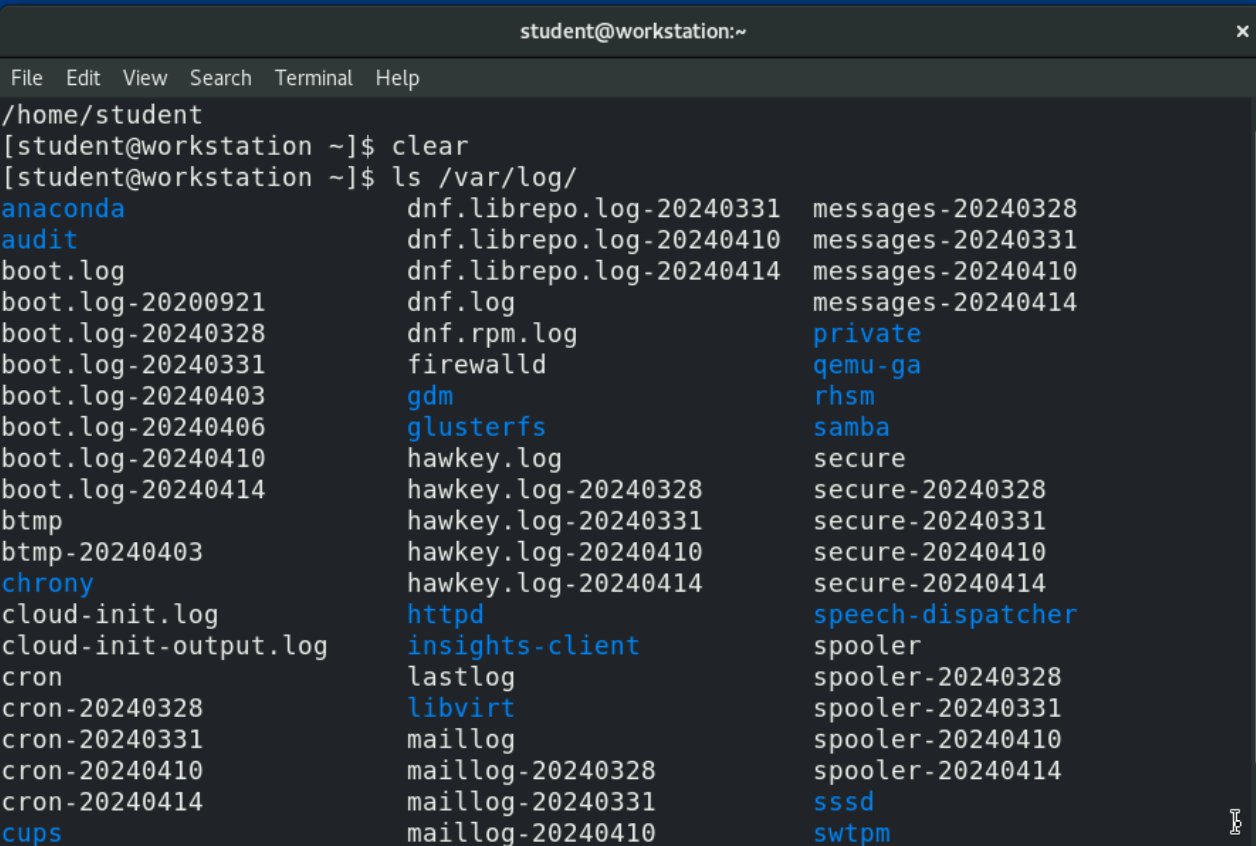
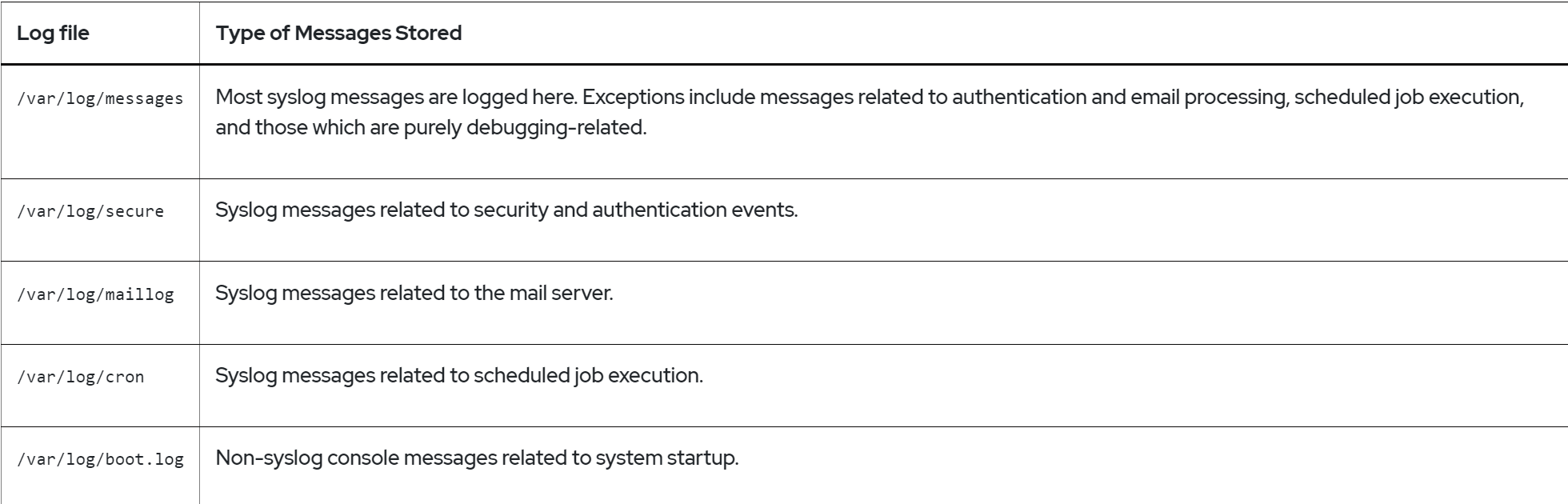
Chapter 11. Analyzing and Storing Logs

When ever we boot the system The sytem will start the log (record the history)

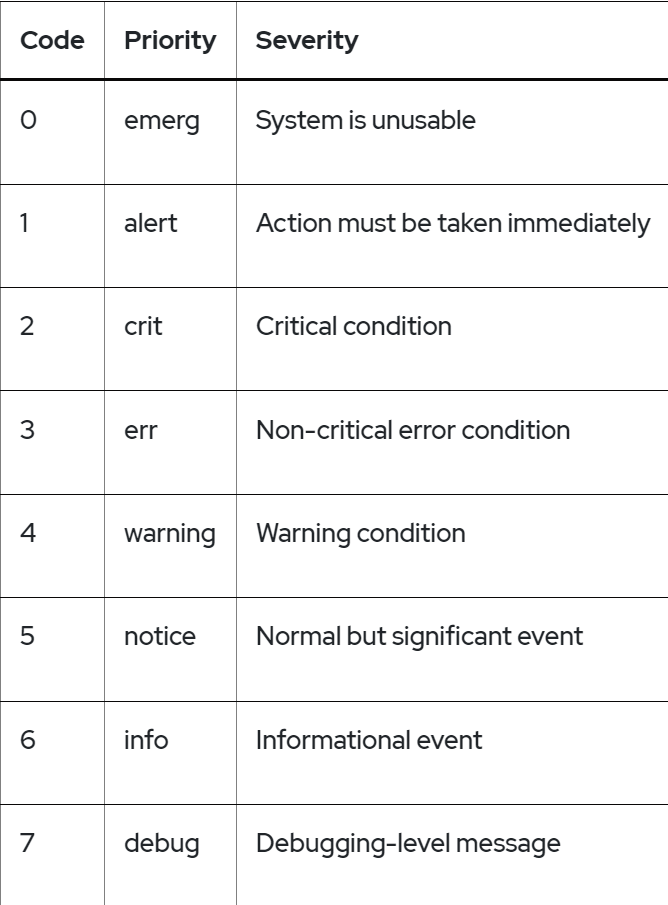


There are file in log (directory)

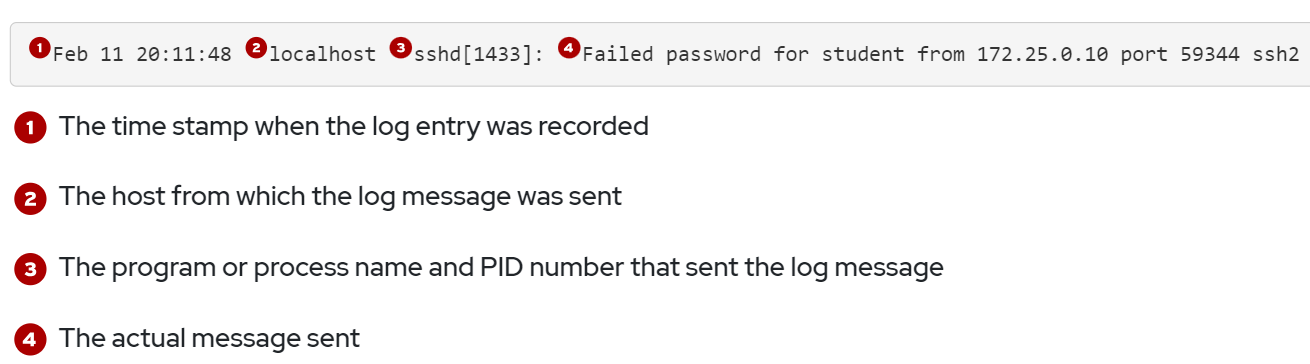
Like:- 

* This jobs are called ‘Crone job’

### Topic:- **Logging Events to the System**

1. **Overview of Syslog Priorities**
   1. 
   2. For example, the following line would record messages sent to the authpriv facility at any priority to the file /var/log/secure:

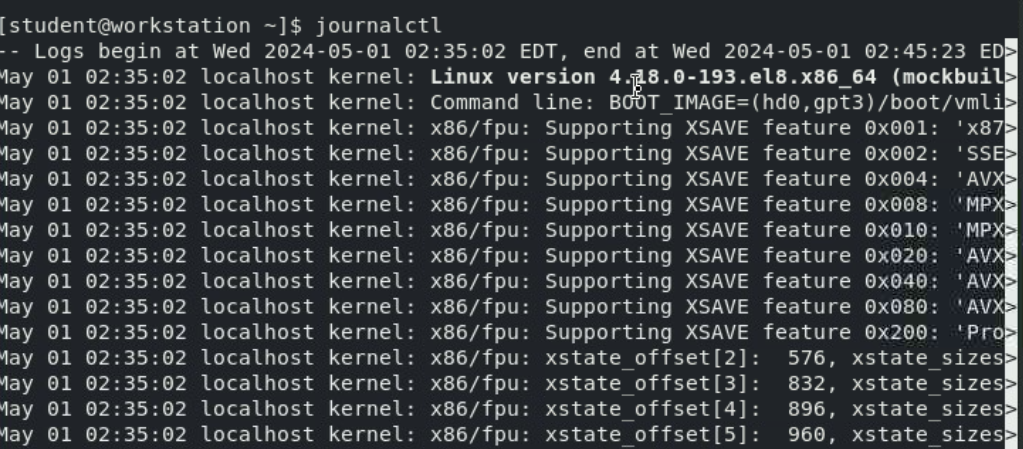
authpriv.\* /var/log/secure

1. **Analyzing a Syslog Entry**
   1. 
   2. The following example explains the anatomy of a log message in the /var/log/secure log file.
2. [take ss form aagam]

### Topic:- **Finding Events**

1. Rsyslog 🡪 permanent storage
   1. Systemd-journald🡪 In memory storage
   2. When the system is closing at that time ‘Systemd-journald’ will send the data to ‘Rsyslog’
   3. And then ‘Rsyslog’ can send the data to other file section
   4. To see this enters :-
      1. Here:-

**[root@host ~]# journalctl**

* + 1. 
    2. Other option is:-