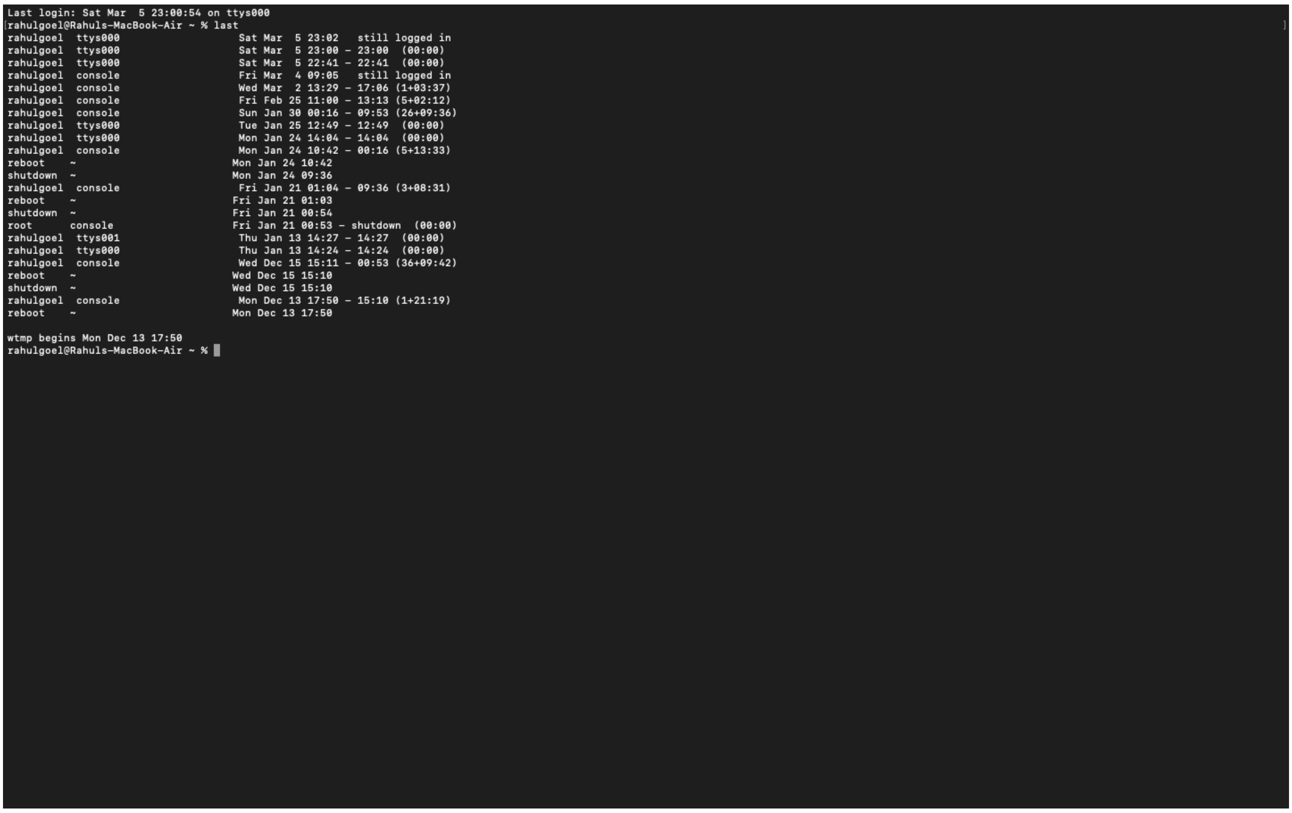
# *CASE STUDY 1: Audit logs*

Reg No: RA1911030010094
Name: Rahul Goel
Forensics and Incident response

Machine : Mac

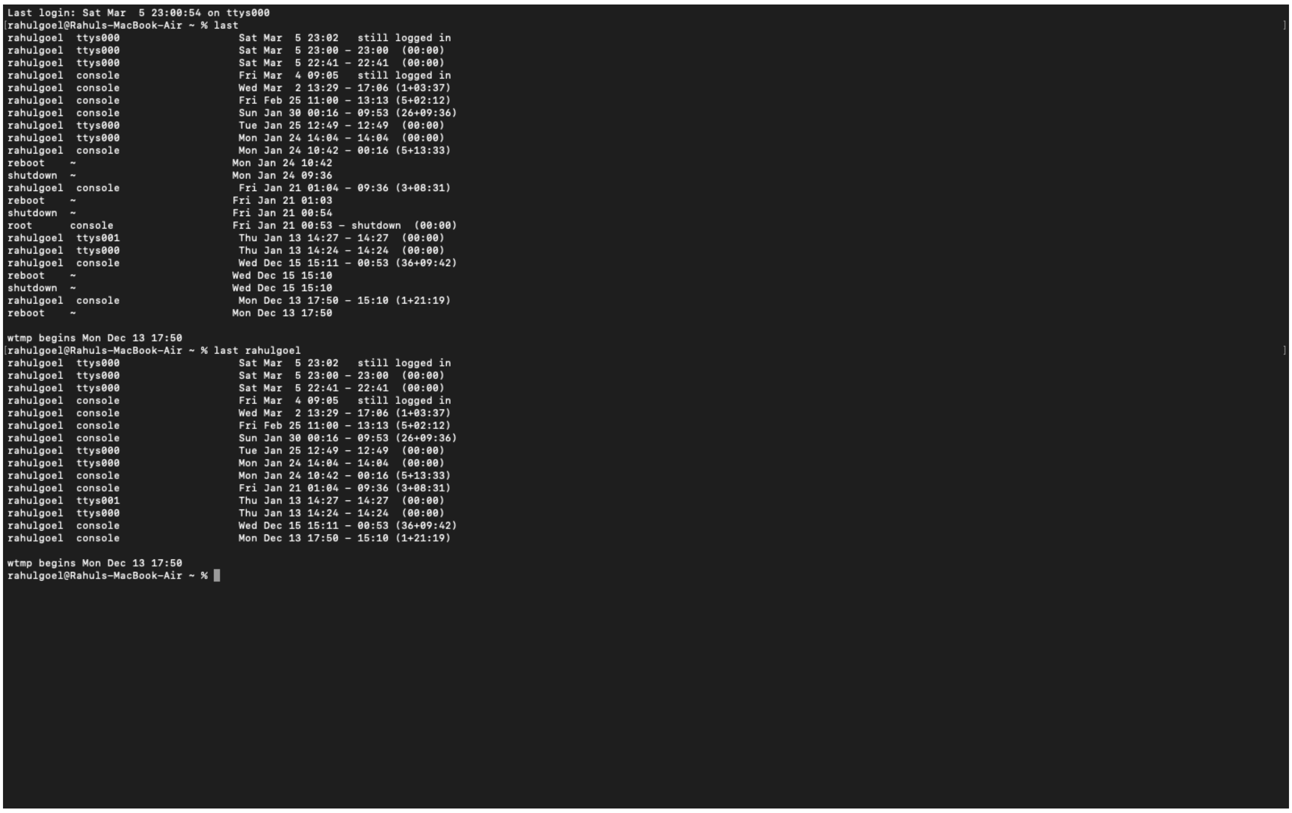
cmd: last --->prints all login logs



```
Last login: Sat Mar  5 23:00:54 on ttys000
rahulgoel@Rahuls-MacBook-Air ~ % last
rahulgoel  ttys000                   Sat Mar  5 23:02   still logged in
rahulgoel  ttys000                   Sat Mar  5 23:00 - 23:00  (00:00)
rahulgoel  ttys000                   Sat Mar  5 22:41 - 22:41  (00:00)
rahulgoel  console                   Fri Mar  4 09:05   still logged in
rahulgoel  console                   Wed Mar  2 13:29 - 17:06 (1+03:37)
rahulgoel  console                   Fri Feb 25 11:00 - 13:13 (5+02:12)
rahulgoel  console                   Sun Jan 30 00:16 - 09:53 (26+09:36)
rahulgoel  ttys000                   Tue Jan 25 12:49 - 12:49  (00:00)
rahulgoel  ttys000                   Mon Jan 24 14:04 - 14:04  (00:00)
rahulgoel  console                   Mon Jan 24 10:42 - 00:16 (5+13:33)
reboot    ~                         Mon Jan 24 10:42
shutdown  ~                         Mon Jan 24 09:36
rahulgoel  console                   Fri Jan 21 01:04 - 09:36 (3+08:31)
reboot    ~                         Fri Jan 21 01:03
shutdown  ~                         Fri Jan 21 00:54
root      console                   Fri Jan 21 00:53 - shutdown  (00:00)
rahulgoel  ttys001                   Thu Jan 13 14:27 - 14:27  (00:00)
rahulgoel  ttys000                   Thu Jan 13 14:24 - 14:24  (00:00)
rahulgoel  console                   Wed Dec 15 15:11 - 00:53 (36+09:42)
reboot    ~                         Wed Dec 15 15:10
shutdown  ~                         Wed Dec 15 15:10
rahulgoel  console                   Mon Dec 13 17:50 - 15:10 (1+21:19)
reboot    ~                         Mon Dec 13 17:50

wtmp begins Mon Dec 13 17:50
rahulgoel@Rahuls-MacBook-Air ~ %
```

cmd: last username -->print logs of that particular user



```
Last login: Sat Mar  5 23:00:54 on ttys000
[rahulgoel@Rahuls-MacBook-Air ~ % last
rahulgoel  ttys000                   Sat Mar  5 23:02   still logged in
rahulgoel  ttys000                   Sat Mar  5 23:00 - 23:00  (00:00)
rahulgoel  ttys000                   Sat Mar  5 22:41 - 22:41  (00:00)
rahulgoel  console                   Fri Mar  4 09:05   still logged in
rahulgoel  console                   Wed Mar  2 13:29 - 17:06 (1+03:37)
rahulgoel  console                   Fri Feb 25 11:00 - 13:13 (5+02:12)
rahulgoel  console                   Sun Jan 30 00:16 - 09:53 (26+09:36)
rahulgoel  ttys000                   Tue Jan 25 12:49 - 12:49  (00:00)
rahulgoel  ttys000                   Mon Jan 24 14:04 - 14:04  (00:00)
rahulgoel  console                   Mon Jan 24 10:42 - 00:16 (5+13:33)
reboot    ~                         Mon Jan 24 10:42
shutdown  ~                         Mon Jan 24 09:36
rahulgoel  console                   Fri Jan 21 01:04 - 09:36 (3+08:31)
reboot    ~                         Fri Jan 21 01:03
shutdown  ~                         Fri Jan 21 00:54
root      console                   Fri Jan 21 00:53 - shutdown  (00:00)
rahulgoel  ttys001                   Thu Jan 13 14:27 - 14:27  (00:00)
rahulgoel  ttys000                   Thu Jan 13 14:24 - 14:24  (00:00)
rahulgoel  console                   Wed Dec 15 15:11 - 00:53 (36+09:42)
reboot    ~                         Wed Dec 15 15:10
shutdown  ~                         Wed Dec 15 15:10
rahulgoel  console                   Mon Dec 13 17:50 - 15:10 (1+21:19)
reboot    ~                         Mon Dec 13 17:50

wtmp begins Mon Dec 13 17:50
[rahulgoel@Rahuls-MacBook-Air ~ % last rahulgoel
rahulgoel  ttys000                   Sat Mar  5 23:02   still logged in
rahulgoel  ttys000                   Sat Mar  5 23:00 - 23:00  (00:00)
rahulgoel  ttys000                   Sat Mar  5 22:41 - 22:41  (00:00)
rahulgoel  console                   Fri Mar  4 09:05   still logged in
rahulgoel  console                   Wed Mar  2 13:29 - 17:06 (1+03:37)
rahulgoel  console                   Fri Feb 25 11:00 - 13:13 (5+02:12)
rahulgoel  console                   Sun Jan 30 00:16 - 09:53 (26+09:36)
rahulgoel  ttys000                   Tue Jan 25 12:49 - 12:49  (00:00)
rahulgoel  ttys000                   Mon Jan 24 14:04 - 14:04  (00:00)
rahulgoel  console                   Mon Jan 24 10:42 - 00:16 (5+13:33)
rahulgoel  console                   Fri Jan 21 01:04 - 09:36 (3+08:31)
rahulgoel  ttys001                   Thu Jan 13 14:27 - 14:27  (00:00)
rahulgoel  ttys000                   Thu Jan 13 14:24 - 14:24  (00:00)
rahulgoel  console                   Wed Dec 15 15:11 - 00:53 (36+09:42)
rahulgoel  console                   Mon Dec 13 17:50 - 15:10 (1+21:19)

wtmp begins Mon Dec 13 17:50
rahulgoel@Rahuls-MacBook-Air ~ % 
```