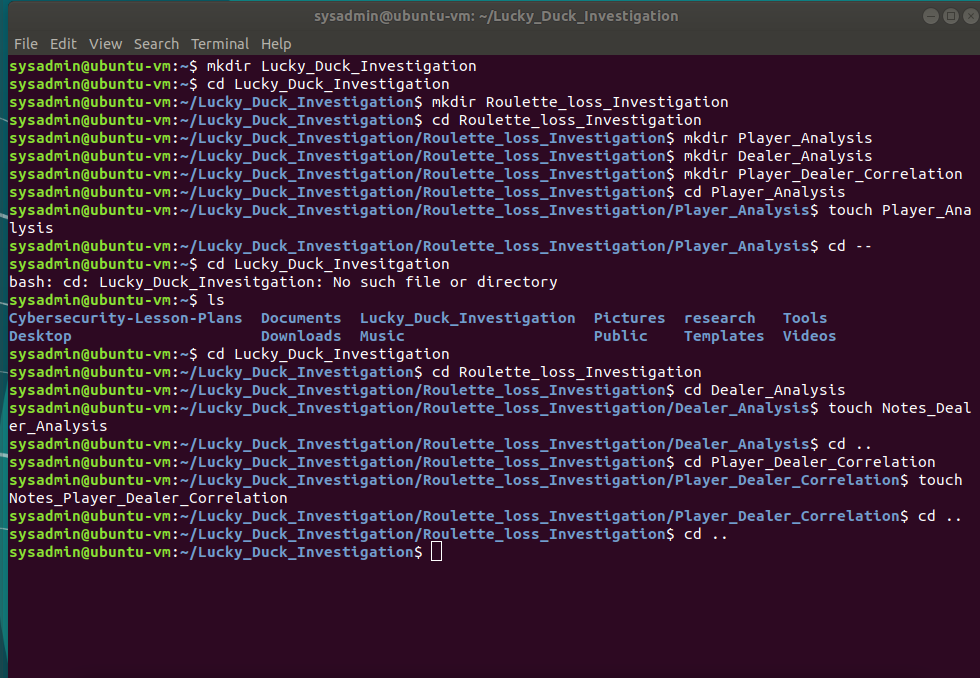
Cybersecurity Homework 3

Step 1: Investigation Preparation

Your first task is to set up directories to prepare for your investigation.

* Begin by making a single directory titled Lucky\_Duck\_Investigations.
* Next, within this directory of Lucky\_Duck\_Investigation, create a directory for this specific investigation titled Roulette\_loss\_Investigation.
* Within Roulette\_loss\_Investigation, create the following directories:
  + Player\_Analysis to investigate the Casino Player.
  + Dealer\_Analysis to investigate the Dealers.
  + Player\_Dealer\_Correlation to summarize your findings of the collusion.
* Create empty files called Notes\_<Directory Name> under each of those subdirectories to be used later to add in any investigation notes.
  + For example: Notes\_Player\_Analysis



Step 2: Gathering Evidence

Your next task is to move evidence from the specific days Lucky Duck experienced heavy losses at the roulette tables.

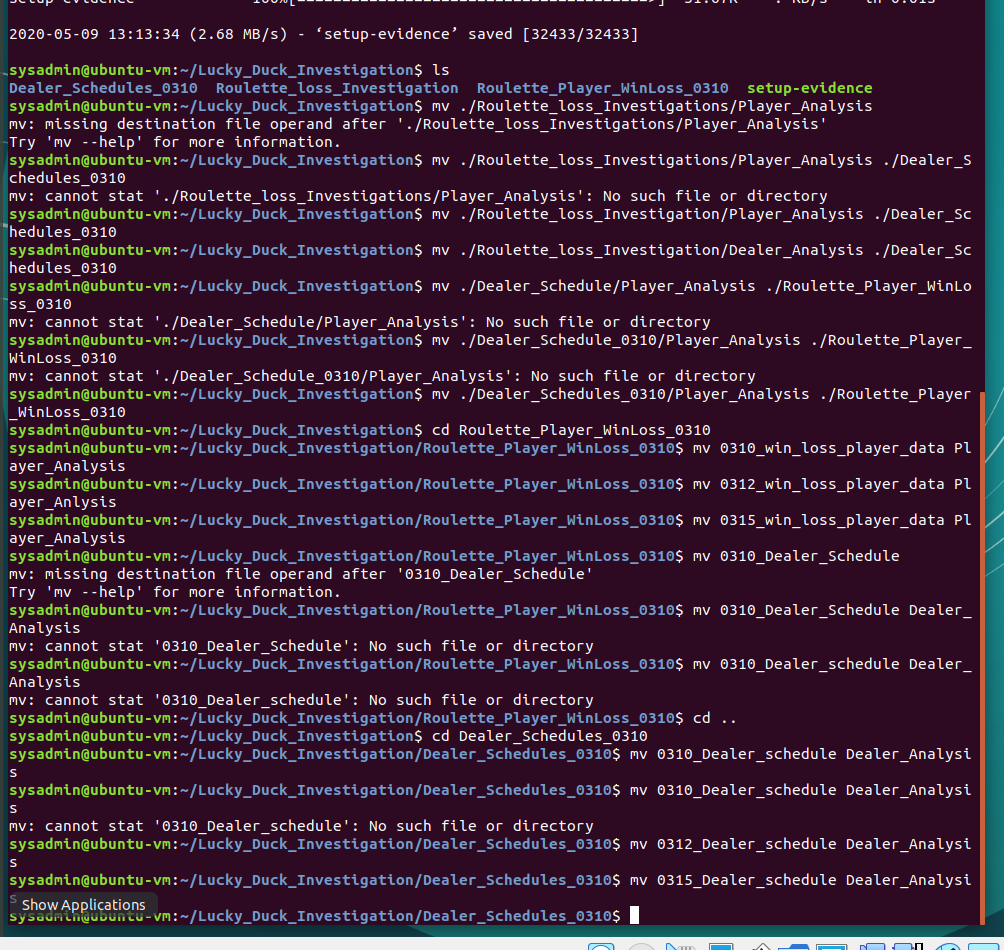
* Navigate to the directory where you created the Lucky\_Duck\_Investigations directory and run the following command to setup the evidence files:

wget "https://tinyurl.com/setup-evidence" && chmod +x ./setup-evidence && ./setup-evidence



After running this command your current directory should have the following subdirectories:

* Dealer\_Schedules\_0310: contains the dealer schedules
* Lucky\_Duck\_Investigations: contains the investigation directories and notes files you created
* Roulette\_Player\_WinLoss\_0310: contains the data for player wins and losses



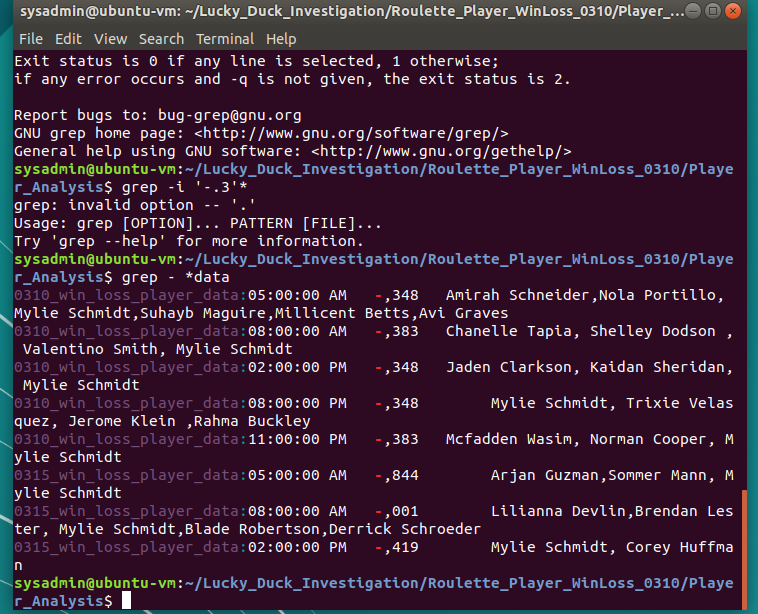
The Dealer\_Schedules\_0310 and Roulette\_Player\_WinLoss\_0310 directories contain the win/loss player data from the roulette tables during the week of March 10th.

* Since the losses occurred on March 10th, 12th, and 15th, move those files into the directory Player\_Analysis.
* Since the losses occurred on March 10th, 12th, and 15th, move the schedules for those days into the directory Dealer\_Analysis

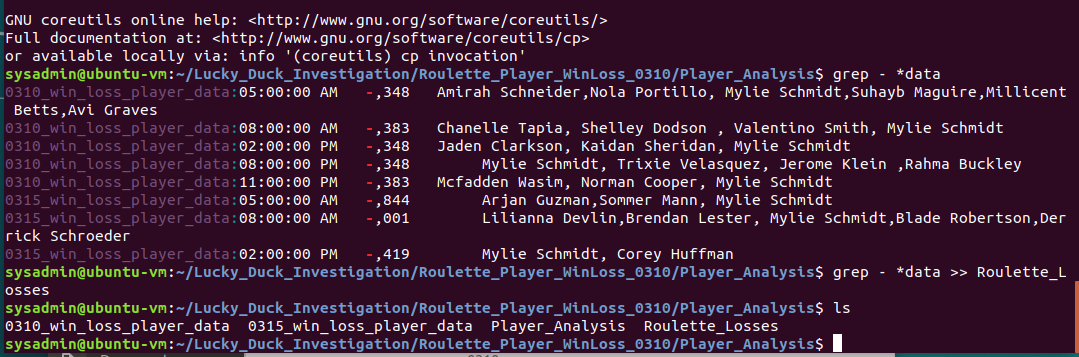
Step 3: Correlating the Evidence

**Player Analysis**

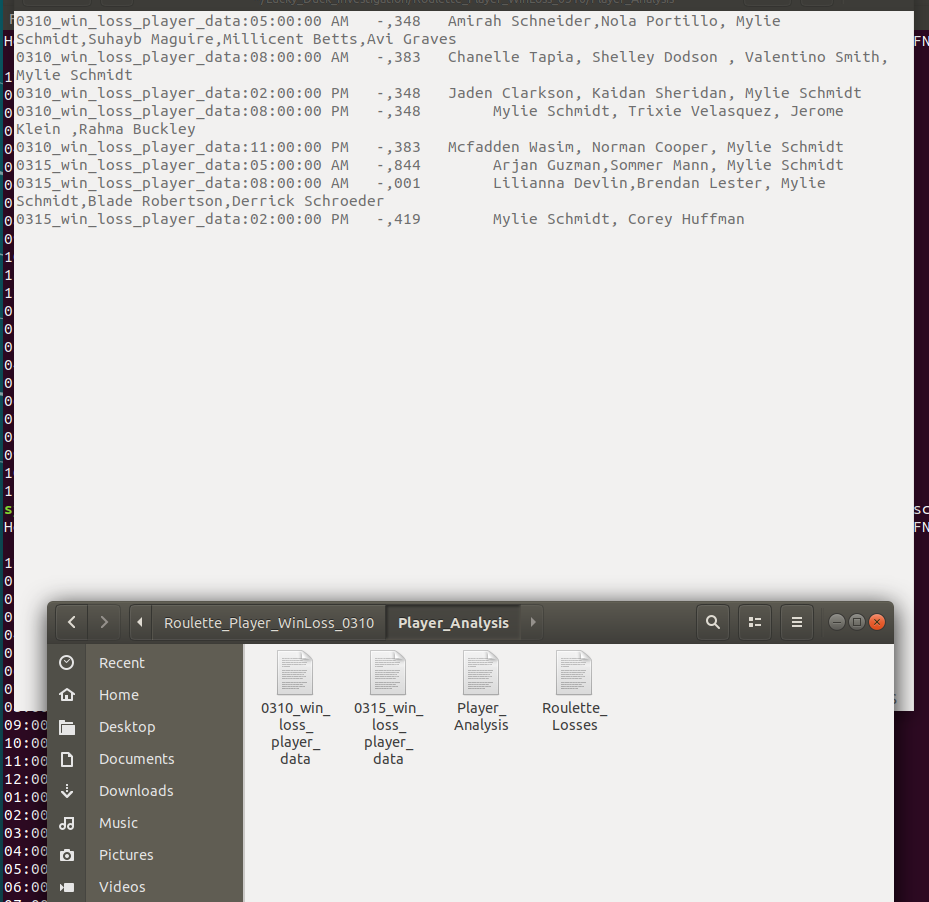
* Navigate to the Player\_Analysis directory.



Use grep to isolate all of the losses that occurred on March 10th, 12th, and 15th.



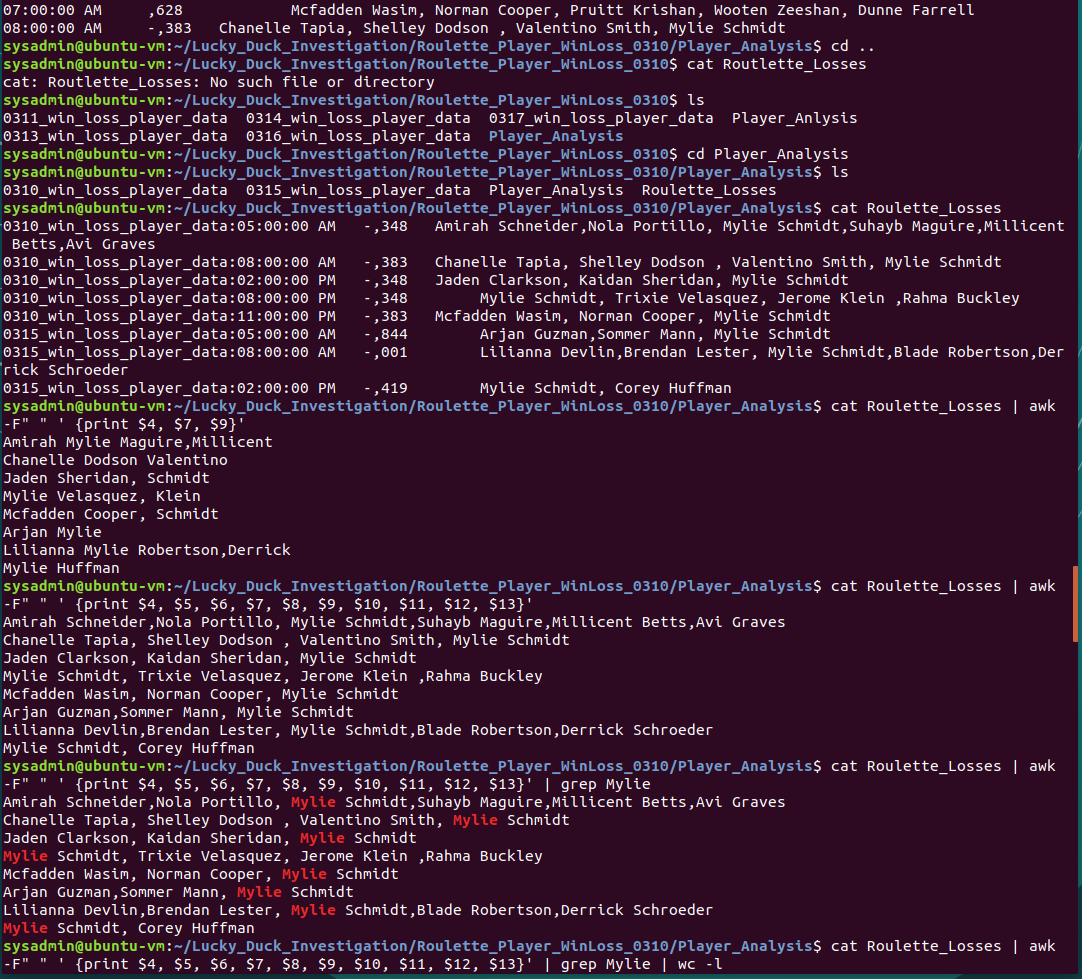
Place those results into a file called Roulette\_Losses.

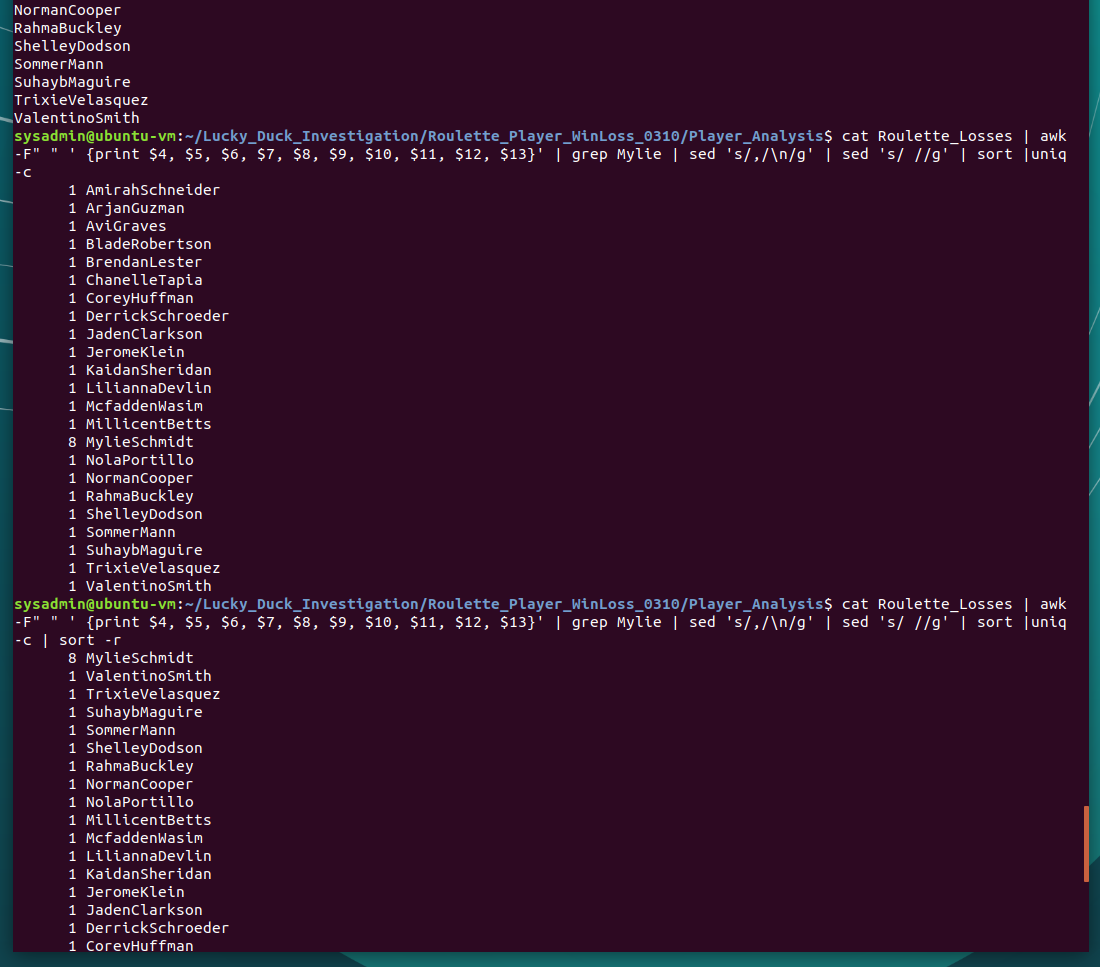


 Preview your file Roulette\_Losses and analyze the data.

 Then, record in the Notes\_Player\_Analysis file:

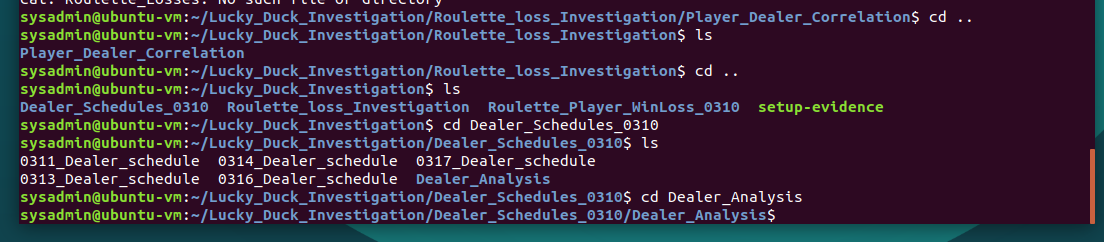
* The times the losses occurred on each day.
* If there is a certain player that was playing during each of those times.
* The total count of times this player was playing.
  + Hint: Use the wc command for this value.





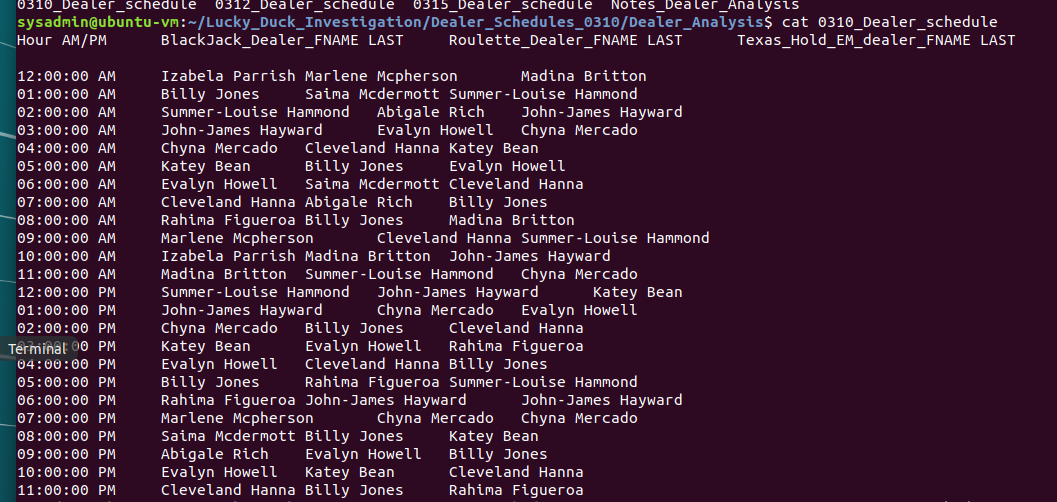
Dealer Analysis

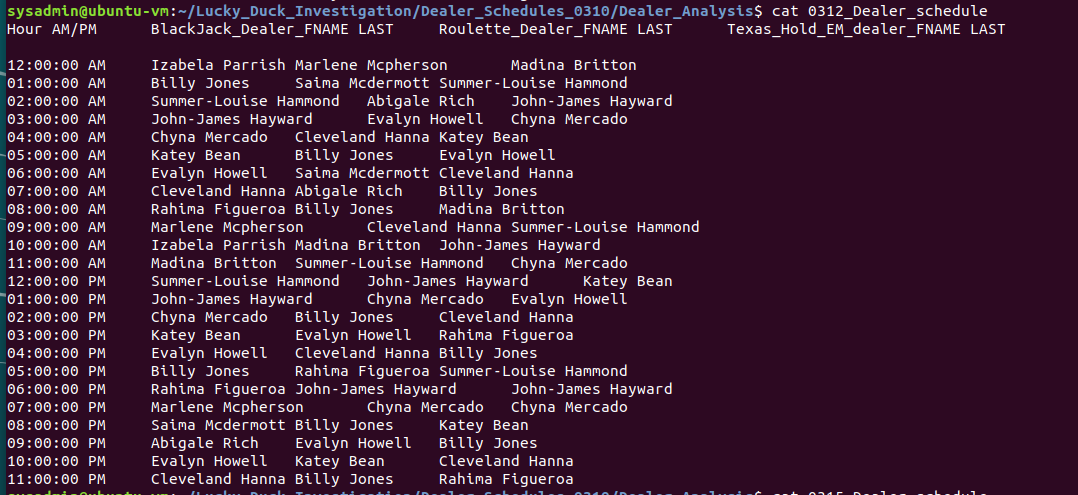
Navigate to the Dealer\_Analysis directory.

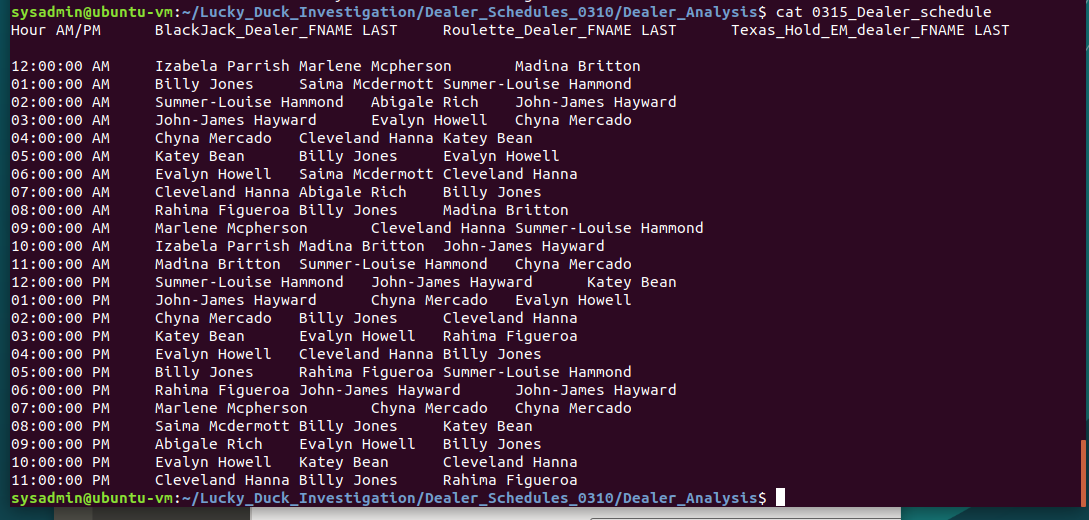


 This file contains the dealer schedules for the various Lucky Duck casino games: Blackjack, Roulette, and Texas Hold 'Em.

 Preview the schedule to view the format and to understand how the data is separated





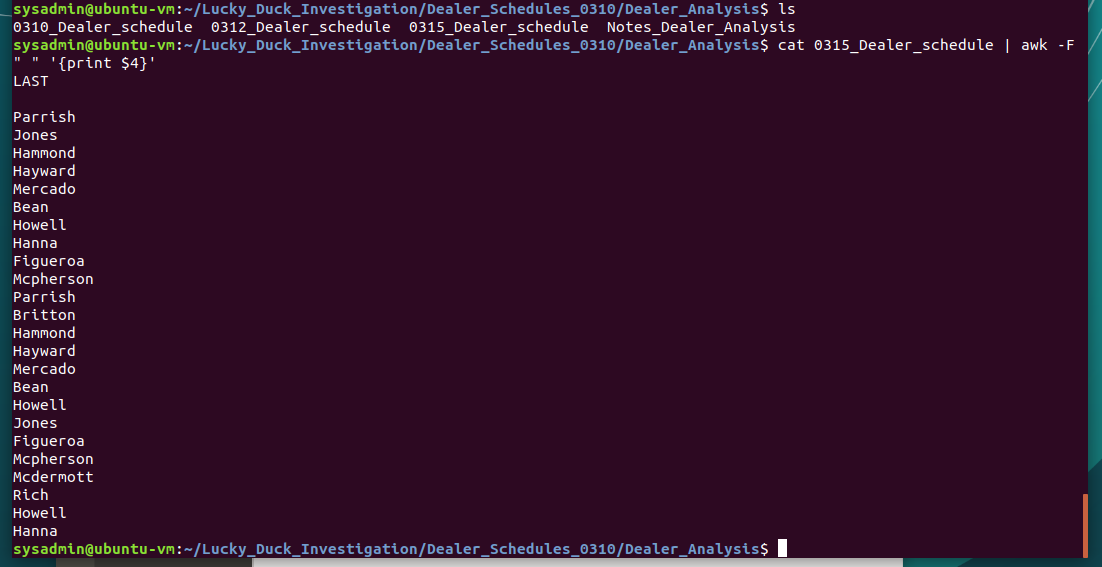


 Using your findings from the player analysis, create a **separate script to look at each day and each time** that you determined where losses occurred. Use awk, pipes, and grep tp isolate out the following four fields:

* Time
* AM/PM
* First name of roulette dealer
* Last name of roulette dealer

 For example, if there was a loss that occurred on March 10th at 2 PM, you would write one script that found the roulette dealer that was working at that specific day and time.

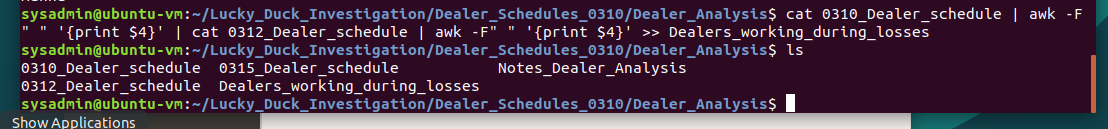
* **Hint**: you will have many scripts, but only a small change is required for each script.







Run all of the scripts and append those results into a file called Dealers\_working\_during\_losses.



Preview your file Dealers\_working\_during\_losses and analyze the data.

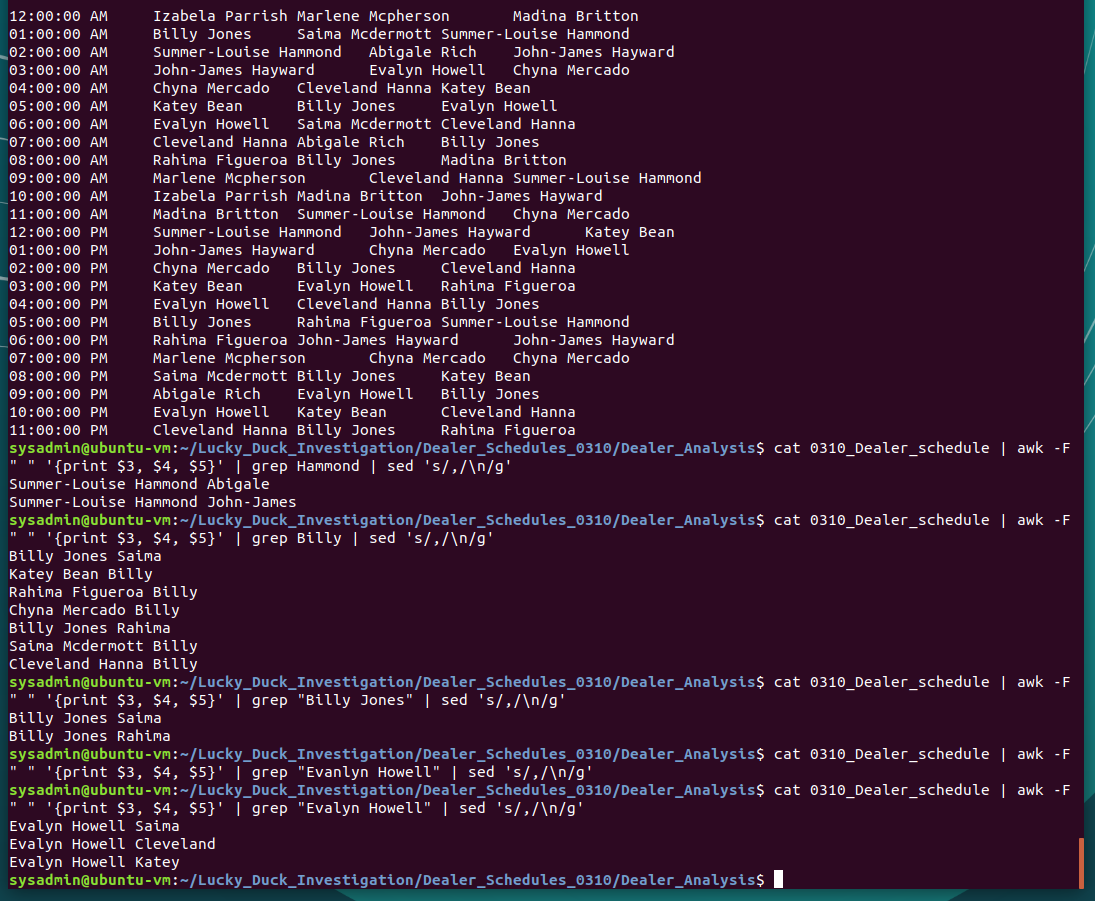
Record in the Notes\_Dealer\_Analysis file:

* The primary dealer working at the times where losses occurred.

Billy Jones

* How many times the dealer worked when major losses occurred.

7



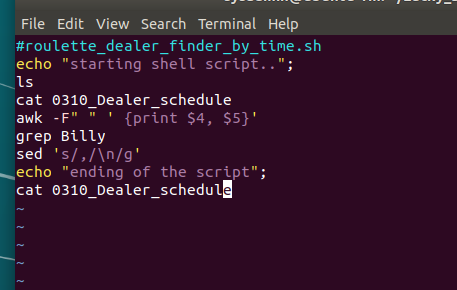
**Step 4: Scripting your Tasks**

You manager is impressed with the work you have done so far on the investigation.

* Your manager has tasked you with building a shell script that can easily analyze future employee schedules. Therefore, we can determine who was the employee working at a specific time in case losses occur again.
* This shell script can be provided to the security department to easily do the same analysis.

Complete the following tasks:

* Remain in the Dealer\_Analysis directory.
* Develop a shell script called roulette\_dealer\_finder\_by\_time.sh that can analyze the employee schedule to easily find the roulette dealer at a specific time.
  + **Hint**: You will be using a script similar to the one you created for the "Dealer Analysis" step, except do not output the results into a file.



* Design the shell script to accept the following two arguments:
  + One for the date (four digits)
  + One for the time

**Note**: The argument should be able to accept AM or PM.

* Test your script on the schedules to confirm it outputs the correct dealer at the time specified.