Step 1: Investigation Preparation

Your first task is to set up directories to prepare for your investigation.
A. Begin by making a single directory titled Lucky_Duck_Investigations
B. In this directory, create a directory for this specific investigation titled Roulette_Loss_Investigation .
C. In 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.
D. Create empty files called Notes_<Directory Name> under each subdirectory to store investigation notes.

Notes: I decided to put the folder into the Desktop location to start and make it easier to organize and view or reference files as needed. The notes and instructions did NOT indicate where they should be placed specifically. Just wanted to make a forward note for this as the class Slack group mentioned to start in the home folder only, vs the instructions of the homework.

Followed all steps above thereafter creating the Lucky_Duck_Investigations folder.
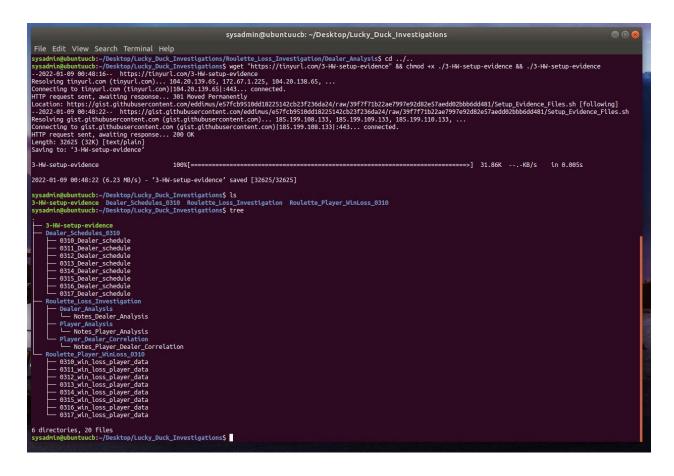
Step 2: Gathering Evidence

1. Navigate to the directory where you created the Lucky_Duck_Investigations directory and run the following command to set up the evidence files:
wget "https://tinyurl.com/3-HW-setup-evidence" && chmod +x ./3-HW-setup-evidence && ./3-HW-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.

Notes: All files downloaded successfully in this step with no issues.

2. The Dealer_Schedules_0310 and Roulette_Player_WinLoss_0310 directories contain the dealer schedules and win/loss player data from the roulette tables during the week of March 10. Since the losses occurred on March 10, 12, and 15, move the schedules for those days into the directory Dealer_Analysis. Move the files for those days into the directory Player_Analysis .
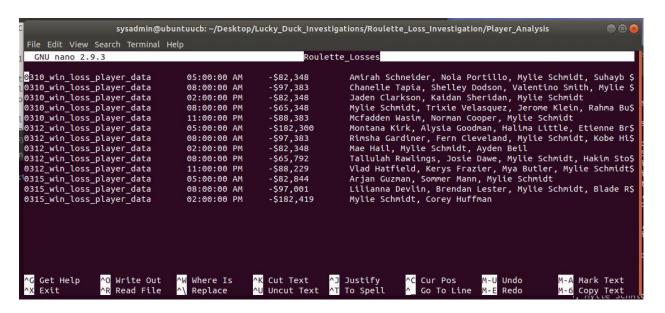
Step 3: Correlating the Evidence

Your next task is to correlate the large losses from the roulette tables with the dealer schedule. This will help you determine which dealer and player are colluding to steal money from Lucky Duck. Note: Winnings for Lucky Duck Casino are indicated with a positive number and losses are indicated with a negative number.

Complete the player analysis.
0. Navigate to the Player_Analysis directory.
1. Use grep to isolate all of the losses that occurred on March 10, 12, and 15.
2. Place those results in a file called Roulette_Losses .
3. Preview the file Roulette_Losses and analyze the data.

Notes: Used grep to search for "-" since all of the losses should have a negative symbol to easily find the lines that were needed for the Roulette_Losses file.

Notes: Used Nano in the following step to make edits to the file formatting. Not all of the data that were taken from the original win loss data was formatted correctly. There are some columns utilizing spaces vs tabs, or there were extra spaces and tabs there making the next step of organizing the data difficult or not work correctly. Some of the commas were also not spaced correctly, and those were adjusted as well.

Record in the Notes_Player_Analysis file:
-The times the losses occurred on each day.

Notes: Used the awk command with the delineator as tab "\t" to output the times, money lost, and players list from the Roulette_Losses file and output the data to Notes_Player_Analysis. Used cat on the file to show the results.

-If there is a certain player that was playing during each of those times.
-The total count of times this player was playing.

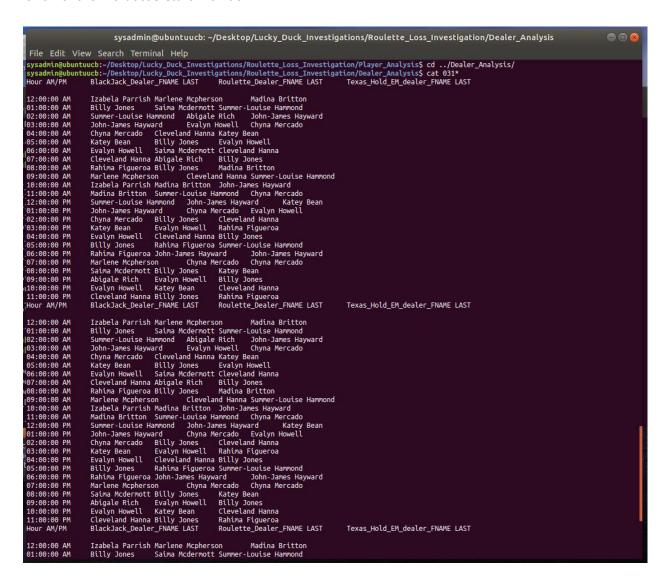*Notes: Decided to used a compounded piped together command to ogranize the data input. Awk the data with the "-F" field set as "tabs" (\t) and then output the column of names in the Roulette_Losses file, which I input to clean up the names with sed by replacing every "," with a "new line" in order to use the sort command. Sorted the data in A-Z order. This allowed me to use the uniq command and "-c" count the number of names that repeated resulting in a count of Mylie Schmidt showing up 13 times.*

Complete the dealer analysis.

0. Navigate to the Dealer_Analysis directory.

1. 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.

<u>Notes:</u> Used the cat command to view all of the files in the folder with 031* as the search term for all of the file dates start with 031.

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

Time

a.m./p.m.

First name of roulette dealer
Last name of roulette dealer

*Notes: Used the grep command to look for ":" since all of the files contained ":" to separate the time numbers and sent all of that data to the file Dealers_Nano to work with further cleaning and organizing the data. The grep allowed me to put all of the files into a single file to pull data from later.

*Notes: In the following side step in organizing the data to be more human readable with all of the schedule information in one file, I used the sed command to substitute all of the file names to a more human readable date file to test the output.

Notes: While continuing my test with the different commands in organizing the data since the human-readable dates worked, I ran a piped a new command with awk to pull just the date, times, and Roulette Dealer only in the file and sent it to a temporary Dealers_RouletteTable file to show just those particular dealer names.

Notes: With all of the data organized, I was able to test and come up with a single grep command for each date to pull the name of the Roulette Dealer in preparation for the script.

Notes: Started a new file in nano to write a grep command for the script. The script(s) were named the respective dates, thus the inputs in the scripts were $1 for the 2 digit time slot and $2 for indicating whether it was AM or PM.

```
cat 0310_Dealer_schedule | awk -F" " '{print $1, $2, $5,$6}'|
grep '08:00:00 AM' >> Dealers_working_during_losses
```

```
sysadmin@ubuntuucb: ~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis

File  Edit  View  Search  Terminal  Help

  GNU nano 2.9.3                        March10RD.sh                         Modified

#!/bin/bash

# This is a script for running March 10's Roulette Dealers

grep "March10:$1:00:00 $2" Dealers_RouletteTable




^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos
^X Exit         ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Linter    ^  Go To Line
```
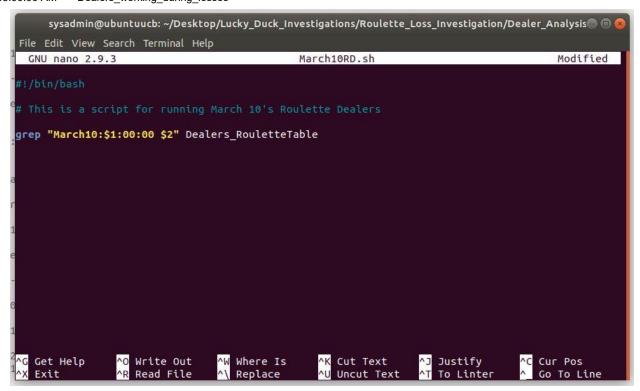
Notes: Saved the script file as the name of the date and closed out nano. Then used chmod to change the mode of the file to an executable file with "chmod +x" for my March10RD.sh script file. Ran a test with the "05" hour and "AM" inputs for the script to make sure it ran correctly.

I then copied the original March10RD.sh for to March12RD.sh and March15RD.sh for the subsequent dates needed. Used nano for each of those files to update the dates in the script to correspond correctly. Have a total of 3 scripts, 1 script for each date.

```
sysadmin@ubuntuucb:~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis$ chmod +x March10RD.sh
sysadmin@ubuntuucb:~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis$ ./March10RD.sh 05 AM
March10:05:00:00 AM Billy Jones
sysadmin@ubuntuucb:~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis$ cp March10RD.sh March12RD.sh
sysadmin@ubuntuucb:~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis$ cp March10RD.sh March15RD.sh
sysadmin@ubuntuucb:~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis$ ^C
sysadmin@ubuntuucb:~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis$ nano March12RD.sh
sysadmin@ubuntuucb:~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis$ nano March15RD.sh
sysadmin@ubuntuucb:~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis$ tree
.
├── 0310_Dealer_schedule
├── 0312_Dealer_schedule
├── 0315_Dealer_schedule
├── Dealers_Nano
├── Dealers_NanoDated
├── Dealers_RouletteTable
├── March10RD.sh
├── March12RD.sh
├── March15RD.sh
└── Notes_Dealer_Analysis

0 directories, 10 files
```

3. Run all of the scripts and append those results to a file called Dealers_working_during_losses.

Notes: Ran all of scripts with the times of the losses seen in the Notes_Player_Analysis file. Appended the outputs with the ">>" to the Dealers_working_during_losses file.

4. Preview your file Dealers_working_during_losses and analyze the data.

Notes: Used cat in the previous screenshot to preview and analyze the data.

Record in the Notes_Dealer_Analysis file:
The primary dealer working at the times where losses occurred.
How many times the dealer worked when major losses occurred.

Notes: Used the awk command to take the column for the First and Last name of the dealers listed in the Dealers_working_during_losses file, then used the "uniq -c" command to count the number of times Billy Jones occurred and sent the data to Notes_Dealer_Analysis.

5. Complete the player/employee correlation.
In the notes file of the Player_Dealer_Correlation directory, add a summary of your findings noting the player and dealer you believe are colluding to scam Lucky Duck. Make sure to document your specific reasons for this finding.

```
                    sysadmin@ubuntuucb: ~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Player_Dealer_Correlation
File Edit View Search Terminal Help
  GNU nano 2.9.3                                   Notes_Player_Dealer_Correlation

After conducting an investigation into the losses of Lucky Duck Casino between the Players and the Dealers, my findings indicate that
there is indeed a Player likely colluding with a Dealer at the Roulette tables to steal money from the casino.

All of the significant loss dates (March 10, 12, and 15) and times provided have a common player named Mylie Schmidt playing at the
Roulette tables.

When comparing those loss dates and times with the Dealer schedules, I have found that Billy Jones has been on shift for all of the times
that Mylie Schmidt has been playing.

All 13 time slots with losses during when Mylie Schmidt was playing match up to the 13 times Billy Jones was on his shift at the Roulette
tables.




                                                            [ Wrote 11 lines ]
^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo        M-A Mark Text   M-] To Bracket
^X Exit         ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell     ^  Go To Line   M-E Redo        M-6 Copy Text   M-W WhereIs Next
```

Step 4: Scripting Your Tasks

Your manager is impressed with the work you have done so far on the investigation.
They tasked you with building a shell script that can easily analyze future employee schedules.
They will use this to determine which employee was working at a specific time in the case of
future losses.

Complete the following tasks:
1. 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.
Design the shell script to accept the following two arguments:
One for the date (four digits)
One for the time

*Notes: Opened up nano for a new script file "roulette_dealer_finder_by_time.sh" and modified
the script to output the name of the dealer working the Roulette table only when you input the
date ($1), time ($2), and whether it was AM or PM ($3). The script then takes the line data of the
grep command to output just the name of the dealer in awk for clarity.*

12

cat $1_Dealer_schedule | awk -F" " '{print $1, $2, $5,$6}'| grep "$2"

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

Notes: Made the new script file executable and then tested the new script with some different dates and it works with outputting the Roulette dealer working that date and time.

Bonus

In case there is future fraud on the other Lucky Duck games, create a shell script called roulette_dealer_finder_by_time_and_game.sh that has the three following arguments:
Specific time
Specific date
Casino game being played

Notes: Since the new script would need to work with new schedules in the future, I've taken the grep command of the last script for the casino to find the the dealers that are working for a specific date and time with all of the schedule files. While trying to explore a possible "if" command to produce a specific dealer given a game, I've discovered the "case" script statement that would allow being able to output specific dealer names for the game given.

WIth this I needed an input command to read data from the command script or, another way was to add the "read" command to take input from the user to choose a game. In this case, I gave the case 3 options for the 3 types of games, and thus titled the read info to the user the 3

different games they could choose from. The "-p" option for prompt would ask the user which game to look at. For the next section, I used the grep command from the last script and piped it together to the case statement to produce the output given the $game selection input from "read."

Each option had the command awk to print out just the columns of the information from the grepped dealer schedule. The times $1 and $2 remained in the same location, but the sections for the dealer names were in separated columns, so $3 and $4 were first names and last name for Blackjack, while $5 and $6 were the first name and last name for the Roulette Dealer.

The "echo" commands used were to space out the lines in the terminal so that they looked cleaner to read.

```
sysadmin@ubuntuucb: ~/Desktop/Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis
File Edit View Search Terminal Help
  GNU nano 2.9.3                          roulette_dealer_finder_by_time_and_game.sh                              Modified

# This is a script that can analyze the employee schedule to easily find the dealer at a specific time and date.
# Inputs: Specific Time, Specific Date, and Casino game being played.

#/bin/bash

echo
echo
read -p "Enter Game Number (1-BlackJack, 2-Roulette, 3-Texas Hold Em): " game
echo
echo
grep -i "$2:00:00 $3" $1_Dealer_schedule |
case "$game" in
        "1") awk '{print " Time: " $1, $2 " Blackjack Dealer: " $3, $4}'
        ;;
        "2") awk '{print " Time: " $1, $2 " Roulette Dealer: " $5, $6}'
        ;;
        "3") awk '{print " Time: " $1, $2 " Texas Hold Em Dealer: " $7, $8}'
        ;;
esac
echo

                                                    [ Read 21 lines ]
^G Get Help    ^O Write Out    ^W Where Is    ^K Cut Text    ^J Justify    ^C Cur Pos     M-U Undo    M-A Mark Text
^X Exit        ^R Read File    ^\ Replace     ^U Uncut Text  ^T To Linter  ^  Go To Line  M-E Redo    M-6 Copy Text
```

Notes: Tested out the new script with the dates, times, and games and it works! See below screenshot.

cat $1_Dealer_schedule | awk -F" " '{print $1, $2, $5,$6}'| grep "$2"