```
sysadmin@UbuntuDesktop:~$ ls
currently_running_processes  Documents  Pictures  Templates
Cybersecurity-Lesson-Plans   Downloads  Public    Videos
Desktop                      Music      python
sysadmin@UbuntuDesktop:~$ mkdir lucky_duck_investigations
sysadmin@UbuntuDesktop:~$ ls
currently_running_processes  Documents                 Music     python
Cybersecurity-Lesson-Plans   Downloads                 Pictures  Templates
Desktop                      lucky_duck_investigations  Public    Videos
sysadmin@UbuntuDesktop:~$ cd lucky_duck_investigations/
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ mkdir roulette_loss_inve
stigation
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ ls
roulette_loss_investigation
```

We begin with our initial setup steps by first creating the “lucky_duck_investigations” directory. Within that, we then make “roulette_loss_investigation” directory

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ mkdir player_analysis ro
ulette_loss_investigation/
mkdir: cannot create directory ‘roulette_loss_investigation/’: File exists
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ mkdir -p roulette_loss_i
nvestigation/player_analysis dealer_analysis player_dealer_correlation
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ tree
.
├── dealer_analysis
├── player_analysis
├── player_dealer_correlation
└── roulette_loss_investigation
    └── player_analysis

5 directories, 0 files
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ ls
dealer_analysis  player_dealer_correlation
player_analysis  roulette_loss_investigation
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ cd roulette_loss_investi
gation/
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigati
on$ cd ..
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ rmdir dealer_analysis pl
ayer_analysis player_dealer_correlation
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ ls
roulette_loss_investigation
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$
```

We then try to make the subsequent directories of “dealer_analysis” “player_analysis” and “player_dealer_correlation” under the “roulette_loss_investigation” directory, but all in one command. The command did not work as I wanted and created directories outside of the desired directory, due to syntax error. I then use “rmdir” to remove the created directories.

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ cd roulette_loss_investi
gation/
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigati
on$ mkdir player_analysis dealer_analysis player_dealer_correlation
mkdir: cannot create directory ‘player_analysis’: File exists
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigati
on$ mkdir dealer_analysis player_dealer_correlation
mkdir: cannot create directory ‘dealer_analysis’: File exists
mkdir: cannot create directory ‘player_dealer_correlation’: File exists
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigati
on$ ls
dealer_analysis  player_analysis  player_dealer_correlation
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigati
on$ tree
.
├── dealer_analysis
├── player_analysis
└── player_dealer_correlation

3 directories, 0 files
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigati
on$
```

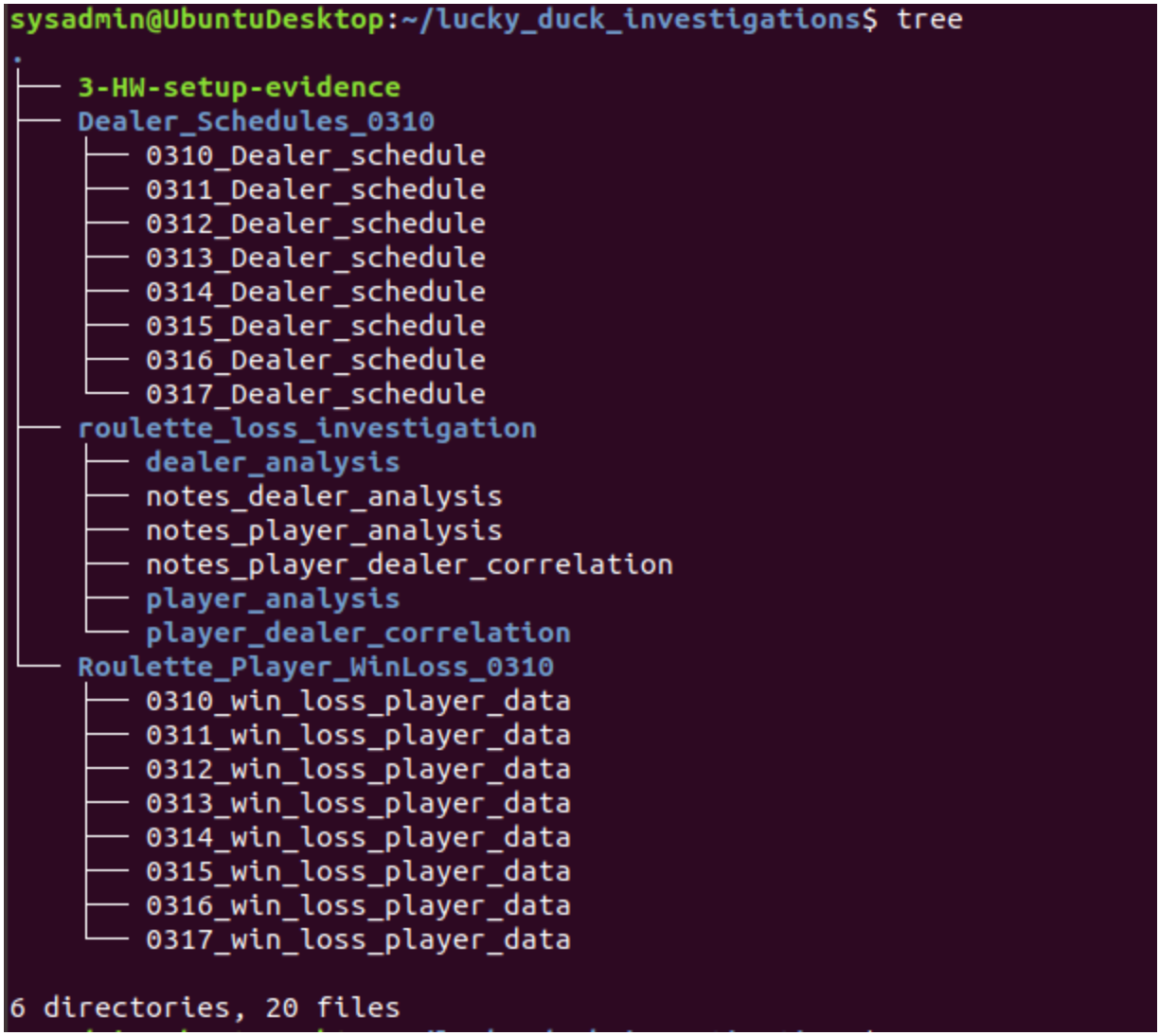
As I try to make the new directories, I discover that the directories already exist, most likely as a result of my previous “mkdir -p” command. Now all files are in place, all that remains is to create note files for each directory.

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigati
on$ touch notes_player_analysis notes_dealer_analysis notes_player_dealer_co
rrelation
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigati
on$ tree
.
├── dealer_analysis
├── notes_dealer_analysis
├── notes_player_analysis
├── notes_player_dealer_correlation
├── player_analysis
└── player_dealer_correlation

3 directories, 3 files
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigati
on$
```

We are now all set up to begin the assignment.

Step 2: Gathering Evidence

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigati
on$ cd ..
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ wget "https://tinyurl.co
m/3-HW-setup-evidence" && chmod +x ./3-HW-setup-evidence && ./3-HW-setup-evi
dence
--2021-10-06 18:07:33--  https://tinyurl.com/3-HW-setup-evidence
Resolving tinyurl.com (tinyurl.com)... 104.20.139.65, 172.67.1.225, 104.20.1
38.65, ...
Connecting to tinyurl.com (tinyurl.com)|104.20.139.65|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://gist.githubusercontent.com/eddimus/e57fcb9510dd18225142cb2
3f236da24/raw/39f7f71b22ae7997e92d82e57aedd02bbb6dd481/Setup_Evidence_Files.
sh [following]
--2021-10-06 18:07:33--  https://gist.githubusercontent.com/eddimus/e57fcb95
10dd18225142cb23f236da24/raw/39f7f71b22ae7997e92d82e57aedd02bbb6dd481/Setup_
Evidence_Files.sh
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199
.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.19
9.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 32625 (32K) [text/plain]
Saving to: ‘3-HW-setup-evidence’

3-HW-setup-evidenc 100%[================>]  31.86K  --.-KB/s    in 0.008s

2021-10-06 18:07:34 (4.09 MB/s) - ‘3-HW-setup-evidence’ saved [32625/32625]
```



We run our wget "https://tinyurl.com/3-HW-setup-evidence" && chmod +x ./3-HW-setup-evidence && ./3-HW-setup-evidence command and then “tree” within the “lucky_duck_unvestigations” directory to confirm the correct execution of the command. We now have all the necessary files to start our analysis.

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/Roulette_Player_WinLoss_0
310$ mv 0310_win_loss_player_data 0312_win_loss_player_data 0315_win_loss_pl
ayer_data ~/lucky_duck_investigations/roulette_loss_investigation/player_ana
lysis/
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/Roulette_Player_WinLoss_0
310$ cd ..
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ tree
.
├── 3-HW-setup-evidence
├── Dealer_Schedules_0310
│   ├── 0310_Dealer_schedule
│   ├── 0311_Dealer_schedule
│   ├── 0312_Dealer_schedule
│   ├── 0313_Dealer_schedule
│   ├── 0314_Dealer_schedule
│   ├── 0315_Dealer_schedule
│   ├── 0316_Dealer_schedule
│   └── 0317_Dealer_schedule
├── roulette_loss_investigation
│   ├── dealer_analysis
│   ├── notes_dealer_analysis
│   ├── notes_player_analysis
│   ├── notes_player_dealer_correlation
│   ├── player_analysis
│   │   ├── 0310_win_loss_player_data
│   │   ├── 0312_win_loss_player_data
│   │   └── 0315_win_loss_player_data
│   └── player_dealer_correlation
└── Roulette_Player_WinLoss_0310
    ├── 0311_win_loss_player_data
    ├── 0313_win_loss_player_data
    ├── 0314_win_loss_player_data
    ├── 0316_win_loss_player_data
    └── 0317_win_loss_player_data
```

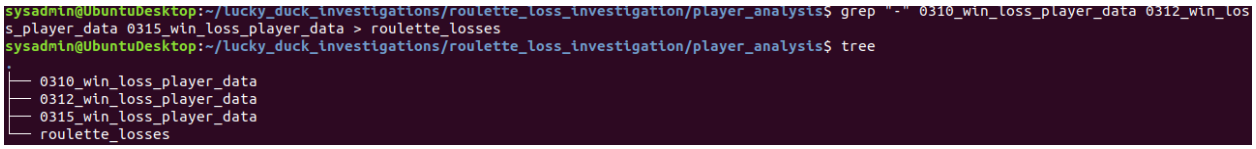
The next step is to move the relevant files of dates March 10, 12, and 15th to “player_analysis” (shown above) and the relevant schedules to “dealer_analysis”. (Shown below)

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/Dealer_Schedules_0310$ mv
 0310_Dealer_schedule 0312_Dealer_schedule 0315_Dealer_schedule ~/lucky_duck
_investigations/roulette_loss_investigation/dealer_analysis/
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/Dealer_Schedules_0310$ cd
 ..
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ trr

Command 'trr' not found, did you mean:

  command 'tr' from deb coreutils
  command 'drr' from deb plastimatch
  command 'tdr' from deb devtodo
  command 'rr' from deb rr
  command 'trn' from deb trn4
  command 'trs' from deb konwert
  command 'tar' from deb tar
  command 'tor' from deb tor

Try: sudo apt install <deb name>

sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ tree
.
├── 3-HW-setup-evidence
├── Dealer_Schedules_0310
│   ├── 0311_Dealer_schedule
│   ├── 0313_Dealer_schedule
│   ├── 0314_Dealer_schedule
│   ├── 0316_Dealer_schedule
│   └── 0317_Dealer_schedule
├── roulette_loss_investigation
│   ├── dealer_analysis
│   │   ├── 0310_Dealer_schedule
│   │   ├── 0312_Dealer_schedule
│   │   └── 0315_Dealer_schedule
│   ├── notes_dealer_analysis
│   ├── notes_player_analysis
│   ├── notes_player_dealer_correlation
│   ├── player_analysis
│   │   ├── 0310_win_loss_player_data
│   │   ├── 0312_win_loss_player_data
│   │   └── 0315_win_loss_player_data
│   └── player_dealer_correlation
└── Roulette_Player_WinLoss_0310
    ├── 0311_win_loss_player_data
    ├── 0313_win_loss_player_data
    ├── 0314_win_loss_player_data
    ├── 0316_win_loss_player_data
    └── 0317_win_loss_player_data

6 directories, 20 files
```

Step 3: Correlating the Evidence

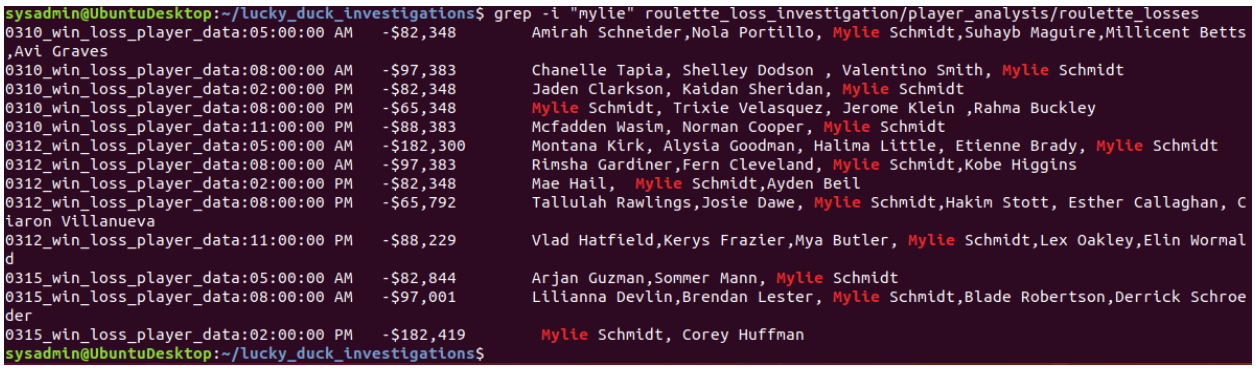
We now need to find and isolate losses which are indicated with a negative number as listed by step 3 notes.

The picture is a bit smaller this time, but sufficient to find the information of all the losses. We now need to turn this into a “roulette_losses” file.



There’s the file in the “player_analysis” directory. Now to check the contents to make sure the command was successful. We can do this with a tail command.

There’s all our data now, ready for analysis. The times the losses have occurred are displayed with the tail command above. But now we need to find a certain player active during those times and how many times they played. A cursory glance of our tail result shows a “Mylie Schmidt” at least twice so we can start there to see if they played at every time there was a loss. For this we will run a grep command for “Mylie”.



Looks like Mylie shows up frequently. Let's find out how many times using a word count command since it's faster than counting.

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ grep -ic "mylie" roulette_loss_investigation/player_analysis/roulette_losses
13
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$
```

Looks like Mylie has played a total of 13 times across each time period the losses occurred. We have our data. Now to place it all in the "notes_player_analysis" file we created earlier. So we're going to run the following:

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ grep -i "mylie" roulette_loss_investigation/player_analysis/roulette_losses > ro
ulette_loss_investigation/notes_player_analysis
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ grep -ic "mylie" roulette_loss_investigation/player_analysis/roulette_losses >>
roulette_loss_investigation/notes_player_analysis
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$
```

We ran grep the first time to get all the time and player data. Then we run grep again with a "-c" option to get the "Mylie" count of 13 added to the file as well. We add it to the file to avoid overwriting the file. Now to just double check the file we will run a "tail" command.

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ tail -20 roulette_loss_investigation/notes_player_analysis
0310_win_loss_player_data:05:00:00 AM   -$82,348        Amirah Schneider,Nola Portillo, Mylie Schmidt,Suhayb Maguire,Millicent Bett
s,Avi Graves
0310_win_loss_player_data:08:00:00 AM   -$97,383        Chanelle Tapia, Shelley Dodson , Valentino Smith, Mylie Schmidt
0310_win_loss_player_data:02:00:00 PM   -$82,348        Jaden Clarkson, Kaidan Sheridan, Mylie Schmidt
0310_win_loss_player_data:08:00:00 PM   -$65,348        Mylie Schmidt, Trixie Velasquez, Jerome Klein ,Rahma Buckley
0310_win_loss_player_data:11:00:00 PM   -$88,383        Mcfadden Wasim, Norman Cooper, Mylie Schmidt
0312_win_loss_player_data:05:00:00 AM   -$182,300       Montana Kirk, Alysia Goodman, Halima Little, Etienne Brady, Mylie Schmidt
0312_win_loss_player_data:08:00:00 AM   -$97,383        Rimsha Gardiner,Fern Cleveland, Mylie Schmidt,Kobe Higgins
0312_win_loss_player_data:02:00:00 PM   -$82,348        Mae Hail,  Mylie Schmidt,Ayden Beil
0312_win_loss_player_data:08:00:00 PM   -$65,792        Tallulah Rawlings,Josie Dawe, Mylie Schmidt,Hakim Stott, Esther Callaghan,
Ciaron Villanueva
0312_win_loss_player_data:11:00:00 PM   -$88,229        Vlad Hatfield,Kerys Frazier,Mya Butler, Mylie Schmidt,Lex Oakley,Elin Worma
ld
0315_win_loss_player_data:05:00:00 AM   -$82,844        Arjan Guzman,Sommer Mann, Mylie Schmidt
0315_win_loss_player_data:08:00:00 AM   -$97,001        Lilianna Devlin,Brendan Lester, Mylie Schmidt,Blade Robertson,Derrick Schro
eder
0315_win_loss_player_data:02:00:00 PM   -$182,419       Mylie Schmidt, Corey Huffman
13
```

There's all the information with "13" in the last row. Now we move to examining the Dealer data.

Part 2 of Step 3:

Let's take a quick look at the Dealer data we have available to us for each "Dealer_schedule". The data will be listed in order starting with March 10th, then 12th, then 15th.

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ tail -30 roulette_loss_investigation/dealer_analysis/0310_Dealer_schedule
Hour AM/PM      BlackJack_Dealer_FNAME LAST     Roulette_Dealer_FNAME LAST      Texas_Hold_EM_dealer_FNAME LAST

12:00:00 AM     Izabela Parrish Marlene Mcpherson       Madina Britton
01:00:00 AM     Billy Jones     Saima Mcdermott Summer-Louise Hammond
02:00:00 AM     Summer-Louise Hammond   Abigale Rich    John-James Hayward
03:00:00 AM     John-James Hayward      Evalyn Howell   Chyna Mercado
04:00:00 AM     Chyna Mercado   Cleveland Hanna Katey Bean
05:00:00 AM     Katey Bean      Billy Jones     Evalyn Howell
06:00:00 AM     Evalyn Howell   Saima Mcdermott Cleveland Hanna
07:00:00 AM     Cleveland Hanna Abigale Rich    Billy Jones
08:00:00 AM     Rahima Figueroa Billy Jones     Madina Britton
09:00:00 AM     Marlene Mcpherson       Cleveland Hanna Summer-Louise Hammond
10:00:00 AM     Izabela Parrish Madina Britton  John-James Hayward
11:00:00 AM     Madina Britton  Summer-Louise Hammond   Chyna Mercado
12:00:00 PM     Summer-Louise Hammond   John-James Hayward      Katey Bean
01:00:00 PM     John-James Hayward      Chyna Mercado   Evalyn Howell
02:00:00 PM     Chyna Mercado   Billy Jones     Cleveland Hanna
03:00:00 PM     Katey Bean      Evalyn Howell   Rahima Figueroa
04:00:00 PM     Evalyn Howell   Cleveland Hanna Billy Jones
05:00:00 PM     Billy Jones     Rahima Figueroa Summer-Louise Hammond
06:00:00 PM     Rahima Figueroa John-James Hayward      John-James Hayward
07:00:00 PM     Marlene Mcpherson       Chyna Mercado   Chyna Mercado
08:00:00 PM     Saima Mcdermott Billy Jones     Katey Bean
09:00:00 PM     Abigale Rich    Evalyn Howell   Billy Jones
10:00:00 PM     Evalyn Howell   Katey Bean      Cleveland Hanna
11:00:00 PM     Cleveland Hanna Billy Jones     Rahima Figueroa
```

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ tail -30 roulette_loss_investigation/dealer_analysis/0312_Dealer_schedule
Hour AM/PM      BlackJack_Dealer_FNAME LAST     Roulette_Dealer_FNAME LAST      Texas_Hold_EM_dealer_FNAME LAST

12:00:00 AM     Izabela Parrish Marlene Mcpherson       Madina Britton
01:00:00 AM     Billy Jones     Saima Mcdermott Summer-Louise Hammond
02:00:00 AM     Summer-Louise Hammond   Abigale Rich    John-James Hayward
03:00:00 AM     John-James Hayward      Evalyn Howell   Chyna Mercado
04:00:00 AM     Chyna Mercado   Cleveland Hanna Katey Bean
05:00:00 AM     Katey Bean      Billy Jones     Evalyn Howell
06:00:00 AM     Evalyn Howell   Saima Mcdermott Cleveland Hanna
07:00:00 AM     Cleveland Hanna Abigale Rich    Billy Jones
08:00:00 AM     Rahima Figueroa Billy Jones     Madina Britton
09:00:00 AM     Marlene Mcpherson       Cleveland Hanna Summer-Louise Hammond
10:00:00 AM     Izabela Parrish Madina Britton  John-James Hayward
11:00:00 AM     Madina Britton  Summer-Louise Hammond   Chyna Mercado
12:00:00 PM     Summer-Louise Hammond   John-James Hayward      Katey Bean
01:00:00 PM     John-James Hayward      Chyna Mercado   Evalyn Howell
02:00:00 PM     Chyna Mercado   Billy Jones     Cleveland Hanna
03:00:00 PM     Katey Bean      Evalyn Howell   Rahima Figueroa
04:00:00 PM     Evalyn Howell   Cleveland Hanna Billy Jones
05:00:00 PM     Billy Jones     Rahima Figueroa Summer-Louise Hammond
06:00:00 PM     Rahima Figueroa John-James Hayward      John-James Hayward
07:00:00 PM     Marlene Mcpherson       Chyna Mercado   Chyna Mercado
08:00:00 PM     Saima Mcdermott Billy Jones     Katey Bean
09:00:00 PM     Abigale Rich    Evalyn Howell   Billy Jones
10:00:00 PM     Evalyn Howell   Katey Bean      Cleveland Hanna
11:00:00 PM     Cleveland Hanna Billy Jones     Rahima Figueroa
```

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ tail -30 roulette_loss_investigation/dealer_analysis/0315_Dealer_schedule
Hour AM/PM      BlackJack_Dealer_FNAME LAST     Roulette_Dealer_FNAME LAST      Texas_Hold_EM_dealer_FNAME LAST

12:00:00 AM     Izabela Parrish Marlene Mcpherson       Madina Britton
01:00:00 AM     Billy Jones     Saima Mcdermott Summer-Louise Hammond
02:00:00 AM     Summer-Louise Hammond   Abigale Rich    John-James Hayward
03:00:00 AM     John-James Hayward      Evalyn Howell   Chyna Mercado
04:00:00 AM     Chyna Mercado   Cleveland Hanna Katey Bean
05:00:00 AM     Katey Bean      Billy Jones     Evalyn Howell
06:00:00 AM     Evalyn Howell   Saima Mcdermott Cleveland Hanna
07:00:00 AM     Cleveland Hanna Abigale Rich    Billy Jones
08:00:00 AM     Rahima Figueroa Billy Jones     Madina Britton
09:00:00 AM     Marlene Mcpherson       Cleveland Hanna Summer-Louise Hammond
10:00:00 AM     Izabela Parrish Madina Britton  John-James Hayward
11:00:00 AM     Madina Britton  Summer-Louise Hammond   Chyna Mercado
12:00:00 PM     Summer-Louise Hammond   John-James Hayward      Katey Bean
01:00:00 PM     John-James Hayward      Chyna Mercado   Evalyn Howell
02:00:00 PM     Chyna Mercado   Billy Jones     Cleveland Hanna
03:00:00 PM     Katey Bean      Evalyn Howell   Rahima Figueroa
04:00:00 PM     Evalyn Howell   Cleveland Hanna Billy Jones
05:00:00 PM     Billy Jones     Rahima Figueroa Summer-Louise Hammond
06:00:00 PM     Rahima Figueroa John-James Hayward      John-James Hayward
07:00:00 PM     Marlene Mcpherson       Chyna Mercado   Chyna Mercado
08:00:00 PM     Saima Mcdermott Billy Jones     Katey Bean
09:00:00 PM     Abigale Rich    Evalyn Howell   Billy Jones
10:00:00 PM     Evalyn Howell   Katey Bean      Cleveland Hanna
11:00:00 PM     Cleveland Hanna Billy Jones     Rahima Figueroa
```

Now we need to craft some scripts that will pull our relevant information of Time, AM/PM, First name, and Last name of the Dealers working the days of the losses. We will do this with separate scripts. For this, we will run the vim command.

```
#!/bin/bash

##Create a script that will display the time, AM/PM, First name, and last name of Roulette Dealer at the time a loss occurred

#A script will be done for each day

#This script is for March 10th

echo "March 10"

awk '/0[58].+AM|(0[28]|11).+PM/ {print $1, $2, $5, $6}' /home/sysadmin/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis/0310_D
ealer_schedule > /home/sysadmin/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis/March10_losses

echo "File saved as March10_losses"
~
```

Here is the first script for March 10th. Now to test it.

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ vim 0310_dealer_losses.sh
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ chmod +x 0310_dealer_losses.sh
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ ./ 0310bash: _xspecs: bad array subscript
^C
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ ./0310_dealer_losses.sh
March 10
File saved as March10_losses
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ ls
0310_dealer_losses.sh  0310_Dealer_schedule  0312_Dealer_schedule  0315_Dealer_schedule  March10_losses
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ cat March10_losses
05:00:00 AM Billy Jones
08:00:00 AM Billy Jones
02:00:00 PM Billy Jones
08:00:00 PM Billy Jones
11:00:00 PM Billy Jones
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$
```

Vim 0310_dealer_losses.sh is our first vim script. We run chmod +x of the script to make it executable. We then run the script to give us the necessary information as part of analysis for March 10th. We cat the March10_loses to check the resulting information and we see Billy Jones is there for all the times. Now for the other two scripts.

```
#!/bin/bash

#Create a script that will display the time, AM/PM, first name, and last name of the Roulette Dealer at the time a loss occurred

#This script is for March 12th

echo "March 12"

awk '/0[58].+AM|(0[28]|11).+PM/ {print $1, $2, $5, $6}' /home/sysadmin/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis/0312_D
ealer_schedule > /home/sysadmin/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis/March12_losses

echo "File saved as March12_losses"
```

There's the second script for March 12, same as the first.

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ vim 0312_dealer_losses.sh
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ chmod +x 0312_dealer_losses.sh
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ ./0312_dealer_losses.sh
March 12
File saved as March12_losses
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ ls
0310_dealer_losses.sh  0310_Dealer_schedule  0312_dealer_losses.sh  0312_Dealer_schedule  0315_Dealer_schedule  March10_losses  March12_losses
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ cat March12_losses
05:00:00 AM Billy Jones
08:00:00 AM Billy Jones
02:00:00 PM Billy Jones
08:00:00 PM Billy Jones
11:00:00 PM Billy Jones
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$
```

So here are the commands and results for the rest of script 2. As you can see, it executed successfully and running cat on the resulting March12_losses gives us Billy Jones once again. We have 10 out of our 13 losses. The last script will give us the remaining 3.

```
#!/bin/bash

#Create a script that will display the time, AM/PM, first name, and last name of the Roulette Dealer at the time a loss occurred

#This script is for March 15th

echo "March 15"

awk '/0[58].+AM|02.+PM/ {print $1, $2, $5, $6}' /home/sysadmin/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis/0315_Dealer_sc
hedule > /home/sysadmin/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis/March15_losses

echo "File saved as March15_losses"
```

Here is the third script with slight modifications to reflect the change in data noted on March 15th's dealer schedule.

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ vim 0315_dealer_losses.sh
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ chmod +x 0315_dealer_losse.sh
chmod: cannot access '0315_dealer_losse.sh': No such file or directory
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ chmod +x 0315_dealer_losses.sh
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ ./0315_dealer_losses.sh
March 15
File saved as March15_losses
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ ls
0310_dealer_losses.sh  0312_dealer_losses.sh  0315_dealer_losses.sh  March10_losses  March15_losses
0310_Dealer_schedule   0312_Dealer_schedule   0315_Dealer_schedule   March12_losses
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ cat March15_losses
05:00:00 AM Billy Jones
08:00:00 AM Billy Jones
02:00:00 PM Billy Jones
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$
```

There are the commands for the final script, showing us the last 3 time stamps of our total 13 evidence of losses that have occurred. Now we're going to cat all the March losses into a file called "dealers_working_during_losses"

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ cat March1* > dealers_working_during_losses
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ ls
0310_dealer_losses.sh  0312_dealer_losses.sh  0315_dealer_losses.sh  dealers_working_during_losses  March12_losses
0310_Dealer_schedule   0312_Dealer_schedule   0315_Dealer_schedule   March10_losses                 March15_losses
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ cat dealers_working_during_losses
05:00:00 AM Billy Jones
08:00:00 AM Billy Jones
02:00:00 PM Billy Jones
08:00:00 PM Billy Jones
11:00:00 PM Billy Jones
05:00:00 AM Billy Jones
08:00:00 AM Billy Jones
02:00:00 PM Billy Jones
08:00:00 PM Billy Jones
11:00:00 PM Billy Jones
05:00:00 AM Billy Jones
08:00:00 AM Billy Jones
02:00:00 PM Billy Jones
```

All 13 incidences of loss have been recorded in the singular dealers_working_during_losses. The separate "March1*_losses" files have been left to keep the information organized via date. We now write notes in "notes_dealer_analysis".

```
Our investigation shows that Dealer Billy Jones was present during all 13 instances of Roulette at the Lucky Duck Casino.

~
~
~
~
~
~
~
~
~
```

We also fill in our deductions from the resulting data in "notes_player_dealer_correlation"

```
So in our investigations, we have deduced 13 total losses involving the player Mylie Schmidt with Billy Jones as the dealer occurring during each o
ne of those instances during a the game of Roulette. This result was achieved by initially identifying whic user was present during the time of eve
ry loss that occurred. The times and dates of this were marked. We then examined which dealer was present during the times that the losses occurred
 and compared them to overlaps in time of the suspected player. 13 incidents were recorded with player Mylie Schmidt and dealer Billy Jones present
 at every instance a loss occurred.
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"roulette_loss_investigation/notes_player_dealer_correlation" 1L, 626C                                                       1,624         All
```

Step 4: Scripting Your Tasks

We now need to put together a script that will analyze the overall employee schedule so that we can find the date, time, and what specific employee is working during that time frame.

```
#!/bin/bash

#This script is to find Specific date and time.

#What do you call an alligator in a vest?

awk -F' ' '{print $1, $2,$'$4',$'$5'}' /home/sysadmin/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis/$1
_Dealer_schedule | grep -i $2"\:00\:00\s"$3m

#An investi"gator"

~
~
~
~
~
~
~
~
~
~
~
~
~
~
"roulette_dealer_finder_by_time_and_game.sh" [New] 11L, 303C written                    11,0-1        All
```

Here is our script. Below, we went ahead and tested the script before making it executable. We then executed the script in the current working directory with a different set of inputs to show that it can find any dealer with the related information.

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ vim roulette_dealer_finder_by_
time_and_game.sh
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ bash roulette_dealer_finder_by
_time_and_game.sh 031[025] 11 p 3 4
11:00:00 PM Cleveland Hanna
11:00:00 PM Cleveland Hanna
11:00:00 PM Cleveland Hanna
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ chmod +x roulette_dealer_finde
r_by_time_and_game.sh
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$ ./roulette_dealer_finder_by_ti
me_and_game.sh 031[025] 11 p 7 8
11:00:00 PM Rahima Figueroa
11:00:00 PM Rahima Figueroa
11:00:00 PM Rahima Figueroa
sysadmin@UbuntuDesktop:~/lucky_duck_investigations/roulette_loss_investigation/dealer_analysis$
```

That about wraps up all of our sleuthing for the Lucky Duck Casino case. Now we copy everything over to “player_dealer_correlation”

```
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ cp roulette_loss_investigation/dealer_analysis/dealers_working_during_los
ses roulette_loss_investigation/player_dealer_correlation/
sysadmin@UbuntuDesktop:~/lucky_duck_investigations$ cp roulette_loss_investigation/player_analysis/roulette_losses roulette_l
oss_investigation/player_dealer_correlation/
```

```
player_dealer_correlation
├── dealers_working_during_losses
└── roulette_losses
```

A quick look at the folder tells us everything is in place. And that concludes the assignment. Happy Hunting!