CIT 383 – Administrative Scripting
Project 5

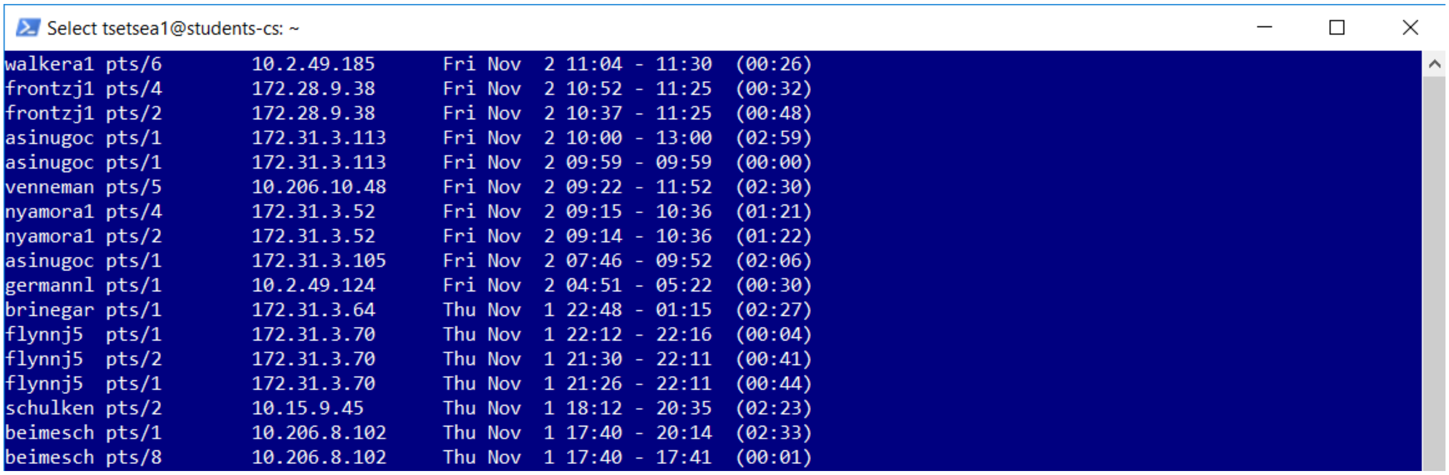
Problem

The security department, of the company that you are currently employed with, is suspicious of some employees. They are requesting a data dump of user login information. You will need to provide to the security department a list of all users who had a successful login.

Overview

This programming assignment is designed to let you practice invoking external commands from Ruby, using hashes, stream I/O, command line options, and (optionally) the CSV standard library methods. It uses the Linux command "last" as the source to produce a report showing who has logged in, how many times, from how many different IP addresses, etc., during the period recorded in the data file /var/log/wtmp or /var/log/wtmp.*n* as determined by the command-line arguments.
First, research the "last" command using the man page. You will find that if you simply type "last," it reads from /var/log/wtmp and shows a listing of all successful logins in reverse chronological order for the period recorded in the current /var/log/wtmp file. The following is a sample run of the "last" command.

Note: By default, the *last* command will return the first 8 characters of the userid. The *getent* command, as you will read below, requires the full userid, not just the first 8 characters. To obtain the complete userid from the *last* command, you must include the –*w* option. Therefore you are to always issue the *last* command as: **last –w**.



```
walkera1 pts/6        10.2.49.185      Fri Nov  2 11:04 - 11:30  (00:26)
frontzj1 pts/4        172.28.9.38      Fri Nov  2 10:52 - 11:25  (00:32)
frontzj1 pts/2        172.28.9.38      Fri Nov  2 10:37 - 11:25  (00:48)
asinugoc pts/1        172.31.3.113     Fri Nov  2 10:00 - 13:00  (02:59)
asinugoc pts/1        172.31.3.113     Fri Nov  2 09:59 - 09:59  (00:00)
venneman pts/5        10.206.10.48     Fri Nov  2 09:22 - 11:52  (02:30)
nyamora1 pts/4        172.31.3.52      Fri Nov  2 09:15 - 10:36  (01:21)
nyamora1 pts/2        172.31.3.52      Fri Nov  2 09:14 - 10:36  (01:22)
asinugoc pts/1        172.31.3.105     Fri Nov  2 07:46 - 09:52  (02:06)
germannl pts/1        10.2.49.124      Fri Nov  2 04:51 - 05:22  (00:30)
brinegar pts/1        172.31.3.64      Thu Nov  1 22:48 - 01:15  (02:27)
flynnj5  pts/1        172.31.3.70      Thu Nov  1 22:12 - 22:16  (00:04)
flynnj5  pts/2        172.31.3.70      Thu Nov  1 21:30 - 22:11  (00:41)
flynnj5  pts/1        172.31.3.70      Thu Nov  1 21:26 - 22:11  (00:44)
schulken pts/2        10.15.9.45       Thu Nov  1 18:12 - 20:35  (02:23)
beimesch pts/1        10.206.8.102     Thu Nov  1 17:40 - 20:14  (02:33)
beimesch pts/8        10.206.8.102     Thu Nov  1 17:40 - 17:41  (00:01)
```

The "last" command has the following options that can be issued as command line arguments:

Option	Description
-i	Translate a FQDN to an IP Address
-f <filename>	Read from a different log file. The default is **/var/log/wtmp**. The –f allows you to specify any previous log file. Of particular interest is the file **/var/log/wtmp.1** which is the previous log generated when the current **wtmp** log is archived by a monthly CRON job. [A system can be configured to store any number of **/var/log/wtmp.*n*** files, but we only have one archived version on students.cs.nku.edu.]

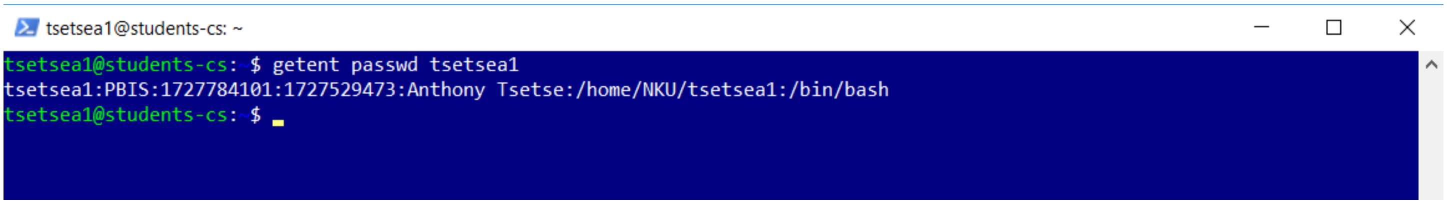
Detailed Requirements

1. The report should include the following information for each user:

Information	Description
Linux user id	The user id that is used to login (ie doej123)
Full Name	The full name of the user (ie John Doe).
Login Date/Time	The most recent login date and time

Total Number of Logins	(self-explanatory)
List of IP Address or FQDNs	Each time the user has logged in, their IPAddress or FQDN (Fully Qualified Doman Name) is recorded.

In order to obtain the full name, you will need to use the "getent" command. Historically, the full name field was known as the "GECOS field" and was used for the full name, office number, etc. You will invoke the "getent" command after obtaining the Linux user id. The following is an example of how to invoke the "getent" command



```
tsetsea1@students-cs: $ getent passwd tsetsea1
tsetsea1:PBIS:1727784101:1727529473:Anthony Tsetse:/home/NKU/tsetsea1:/bin/bash
tsetsea1@students-cs: $
```

Notice that the full name is fifth of the **:** separated fields in the output. If there is no record returned for a user, leave it as a blank (nil).

2. Each user's information shall be on a single line. Meaning, if the report lists 5 users, then there will be 5 lines of information.

3. The report's output should be generated in CSV format such that if we redirect the output of the Ruby script using > in the shell or supply an output file name, the CSV file will be saved and can be transferred to a PC running Microsoft Excel and saved as a spreadsheet.

4. The Ruby program will have the following Command-line options and must be managed using the optparse library:
    - -i : pass-through to the "last" command, telling it to convert FQDNs to IP addresses
    - -f <filename> : pass-through to the "last" command, telling to it read from a specific wtmp file
    - -o <filename> : send the report output to the named file
    - -h : show the command usage summary

Program Flow

1. Create a user hash that will store the user information. This will be your information store.
2. (15 points) Parse the Command-line options.
3. (10 points) Invoke the "last" command passing any command-line arguments.
4. Loop through each line of data that was produced by the "last" command.
5. With each iteration do the following:
    a. Split the line of data to obtain key information.
    This can be done by using the .split() method
    b. Check to see if the Linux user id has been processed before.
    If not, do the following:
        i. (10 points) Using the Linux user id, invoke the "getent" command to get the Full Name.
        Again, split the information using the necessary token.
        ii. (10 points) Capture the Linux user id, full name, and the login date/time
        iii. Store the user information to your information store.
    c. Since every line in the "last" command represents a user login, using your information store, lookup by the Linux user id. Note: This will be done every time, so for part 5.b you should set some default values.
    Do the following:
        i. (10 points) Increment the Total Login Count
        ii. (10 points) Append the IP Address / FQDN to the user's list.

6. Once completed, iterate through the list of users.
   Do the following:
   a. (10 points) Output report in CSV format.
      Output will either be to the console, or if the –o option is present to the output file.

Additional Information

1. (10 points) Your program should run as expected, so Basic Syntax and Runtime Behavior will be enforced.
2. (5 points)The final two lines of the "last" command are a blank line and a summary line stating when the file was started (generally the 1st of the month):

   ```
   wtmp begins Sun Nov  1 10:38:55 2015
   ```

   When parsing the output from the "last" command, you will need to skip over the last two lines. The following regular expression will allow you to do so.

   ```
   next if line =~ /^wtmp*/ || line =~ /^$/
   ```

3. (10 points) General programming style, such as comments, indentation and variable names, will be applied.

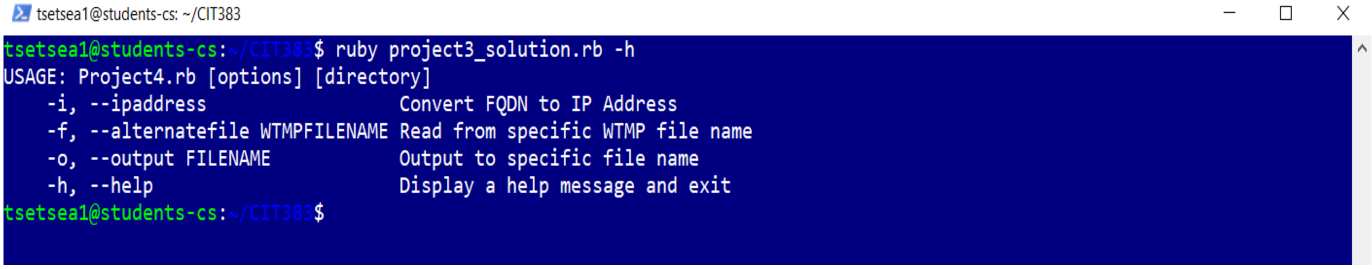
Project Information

Save and Execute file

1. Save your Ruby file, using the file name: **Project3.rb**
2. Upload to linux server (if needed)
3. Execute your ruby script either explicitly or implicitly.
4. Upload your file to Canvas.

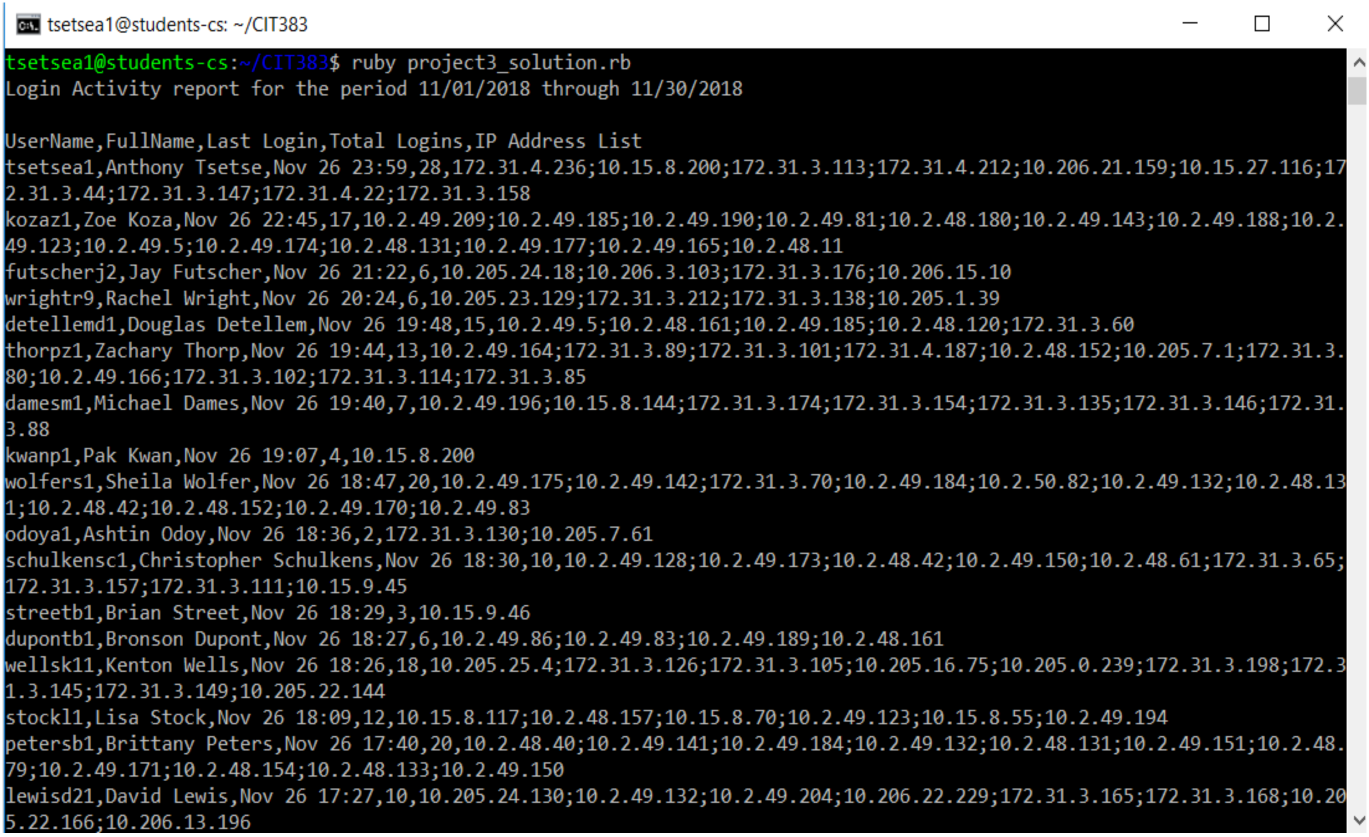
Sample Runs shows Extra Credit

Display help



```
tsetsea1@students-cs:~/CIT383$ ruby project3_solution.rb -h
USAGE: Project4.rb [options] [directory]
    -i, --ipaddress                  Convert FQDN to IP Address
    -f, --alternatefile WTMPFILENAME Read from specific WTMP file name
    -o, --output FILENAME            Output to specific file name
    -h, --help                       Display a help message and exit
tsetsea1@students-cs:~/CIT383$
```

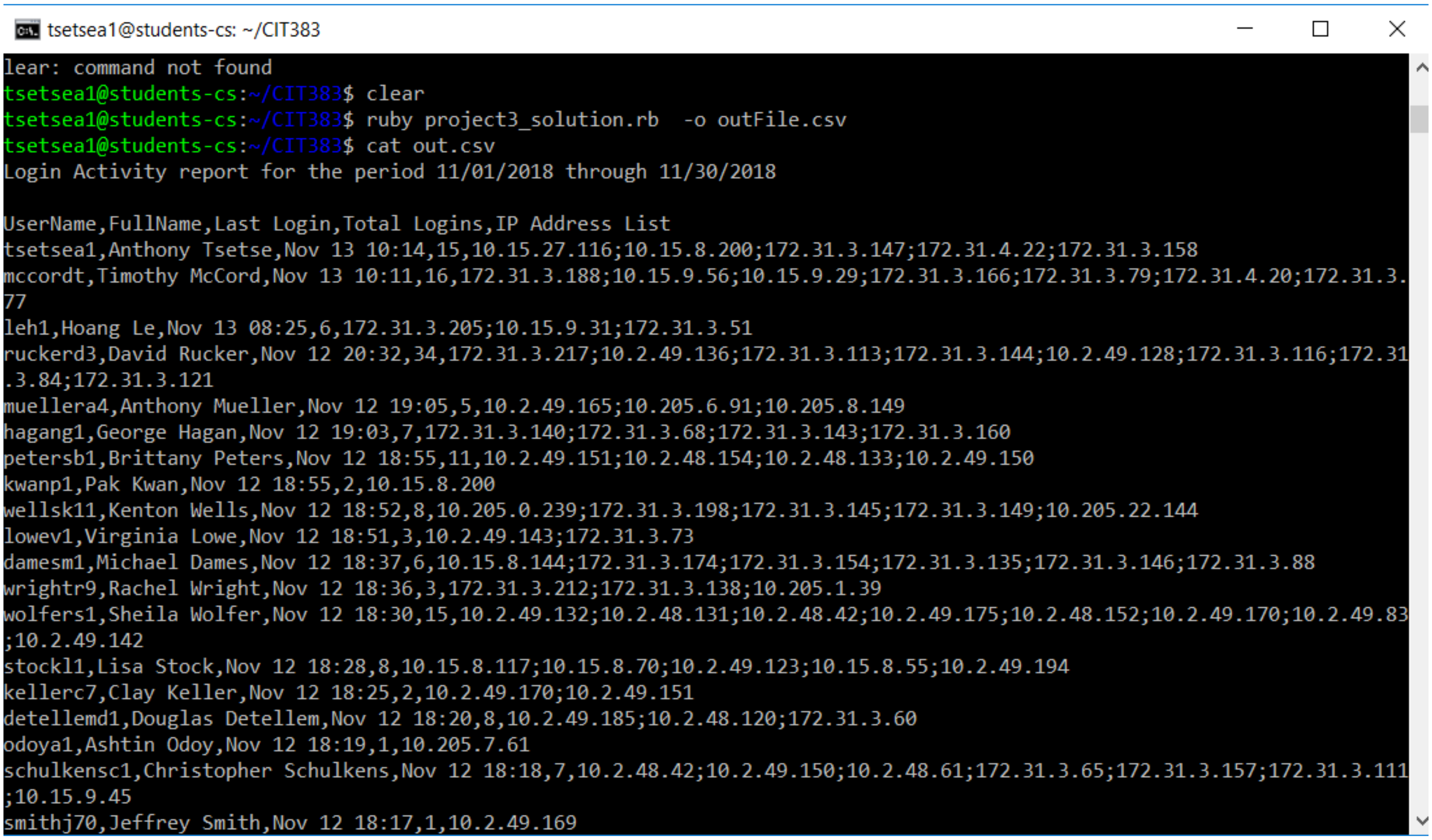
Run with no options (outputs to screen)



```
tsetsea1@students-cs:~/CIT383$ ruby project3_solution.rb
Login Activity report for the period 11/01/2018 through 11/30/2018

UserName,FullName,Last Login,Total Logins,IP Address List
tsetsea1,Anthony Tsetse,Nov 26 23:59,28,172.31.4.236;10.15.8.200;172.31.3.113;172.31.4.212;10.206.21.159;10.15.27.116;17
2.31.3.44;172.31.3.147;172.31.4.22;172.31.3.158
kozaz1,Zoe Koza,Nov 26 22:45,17,10.2.49.209;10.2.49.185;10.2.49.190;10.2.49.81;10.2.48.180;10.2.49.143;10.2.49.188;10.2.
49.123;10.2.49.5;10.2.49.174;10.2.48.131;10.2.49.177;10.2.49.165;10.2.48.11
futscherj2,Jay Futscher,Nov 26 21:22,6,10.205.24.18;10.206.3.103;172.31.3.176;10.206.15.10
wrightr9,Rachel Wright,Nov 26 20:24,6,10.205.23.129;172.31.3.212;172.31.3.138;10.205.1.39
detellemd1,Douglas Detellem,Nov 26 19:48,15,10.2.49.5;10.2.48.161;10.2.49.185;10.2.48.120;172.31.3.60
thorpz1,Zachary Thorp,Nov 26 19:44,13,10.2.49.164;172.31.3.89;172.31.3.101;172.31.4.187;10.2.48.152;10.205.7.1;172.31.3.
80;10.2.49.166;172.31.3.102;172.31.3.114;172.31.3.85
damesm1,Michael Dames,Nov 26 19:40,7,10.2.49.196;10.15.8.144;172.31.3.174;172.31.3.154;172.31.3.135;172.31.3.146;172.31.
3.88
kwanp1,Pak Kwan,Nov 26 19:07,4,10.15.8.200
wolfers1,Sheila Wolfer,Nov 26 18:47,20,10.2.49.175;10.2.49.142;172.31.3.70;10.2.49.184;10.2.50.82;10.2.49.132;10.2.48.13
1;10.2.48.42;10.2.48.152;10.2.49.170;10.2.49.83
odoya1,Ashtin Odoy,Nov 26 18:36,2,172.31.3.130;10.205.7.61
schulkensc1,Christopher Schulkens,Nov 26 18:30,10,10.2.49.128;10.2.49.173;10.2.48.42;10.2.49.150;10.2.48.61;172.31.3.65;
172.31.3.157;172.31.3.111;10.15.9.45
streetb1,Brian Street,Nov 26 18:29,3,10.15.9.46
dupontb1,Bronson Dupont,Nov 26 18:27,6,10.2.49.86;10.2.49.83;10.2.49.189;10.2.48.161
wellsk11,Kenton Wells,Nov 26 18:26,18,10.205.25.4;172.31.3.126;172.31.3.105;10.205.16.75;10.205.0.239;172.31.3.198;172.3
1.3.145;172.31.3.149;10.205.22.144
stockl1,Lisa Stock,Nov 26 18:09,12,10.15.8.117;10.2.48.157;10.15.8.70;10.2.49.123;10.15.8.55;10.2.49.194
petersb1,Brittany Peters,Nov 26 17:40,20,10.2.48.40;10.2.49.141;10.2.49.184;10.2.49.132;10.2.48.131;10.2.49.151;10.2.48.
79;10.2.49.171;10.2.48.154;10.2.48.133;10.2.49.150
lewisd21,David Lewis,Nov 26 17:27,10,10.205.24.130;10.2.49.132;10.2.49.204;10.206.22.229;172.31.3.165;172.31.3.168;10.20
5.22.166;10.206.13.196
```

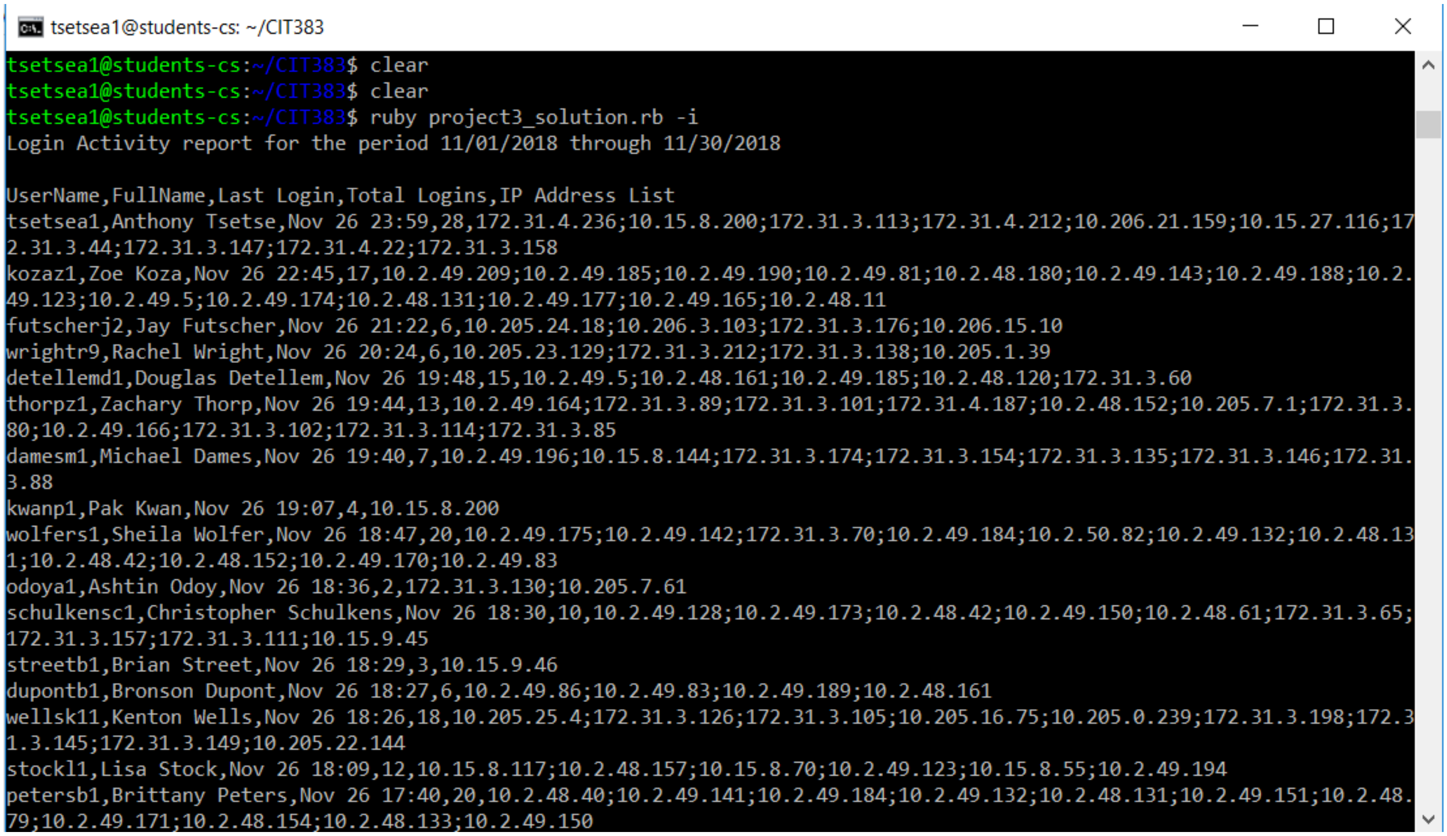
Run using –o option to output to a file



```
lear: command not found
tsetsea1@students-cs:~/CIT383$ clear
tsetsea1@students-cs:~/CIT383$ ruby project3_solution.rb  -o outFile.csv
tsetsea1@students-cs:~/CIT383$ cat out.csv
Login Activity report for the period 11/01/2018 through 11/30/2018

UserName,FullName,Last Login,Total Logins,IP Address List
tsetsea1,Anthony Tsetse,Nov 13 10:14,15,10.15.27.116;10.15.8.200;172.31.3.147;172.31.4.22;172.31.3.158
mccordt,Timothy McCord,Nov 13 10:11,16,172.31.3.188;10.15.9.56;10.15.9.29;172.31.3.166;172.31.3.79;172.31.4.20;172.31.3.
77
leh1,Hoang Le,Nov 13 08:25,6,172.31.3.205;10.15.9.31;172.31.3.51
ruckerd3,David Rucker,Nov 12 20:32,34,172.31.3.217;10.2.49.136;172.31.3.113;172.31.3.144;10.2.49.128;172.31.3.116;172.31
.3.84;172.31.3.121
muellera4,Anthony Mueller,Nov 12 19:05,5,10.2.49.165;10.205.6.91;10.205.8.149
hagang1,George Hagan,Nov 12 19:03,7,172.31.3.140;172.31.3.68;172.31.3.143;172.31.3.160
petersb1,Brittany Peters,Nov 12 18:55,11,10.2.49.151;10.2.48.154;10.2.48.133;10.2.49.150
kwanp1,Pak Kwan,Nov 12 18:55,2,10.15.8.200
wellsk11,Kenton Wells,Nov 12 18:52,8,10.205.0.239;172.31.3.198;172.31.3.145;172.31.3.149;10.205.22.144
lowev1,Virginia Lowe,Nov 12 18:51,3,10.2.49.143;172.31.3.73
damesm1,Michael Dames,Nov 12 18:37,6,10.15.8.144;172.31.3.174;172.31.3.154;172.31.3.135;172.31.3.146;172.31.3.88
wrightr9,Rachel Wright,Nov 12 18:36,3,172.31.3.212;172.31.3.138;10.205.1.39
wolfers1,Sheila Wolfer,Nov 12 18:30,15,10.2.49.132;10.2.48.131;10.2.48.42;10.2.49.175;10.2.48.152;10.2.49.170;10.2.49.83
;10.2.49.142
stockl1,Lisa Stock,Nov 12 18:28,8,10.15.8.117;10.15.8.70;10.2.49.123;10.15.8.55;10.2.49.194
kellerc7,Clay Keller,Nov 12 18:25,2,10.2.49.170;10.2.49.151
detellemd1,Douglas Detellem,Nov 12 18:20,8,10.2.49.185;10.2.48.120;172.31.3.60
odoya1,Ashtin Odoy,Nov 12 18:19,1,10.205.7.61
schulkensc1,Christopher Schulkens,Nov 12 18:18,7,10.2.48.42;10.2.49.150;10.2.48.61;172.31.3.65;172.31.3.157;172.31.3.111
;10.15.9.45
smithj70,Jeffrey Smith,Nov 12 18:17,1,10.2.49.169
```

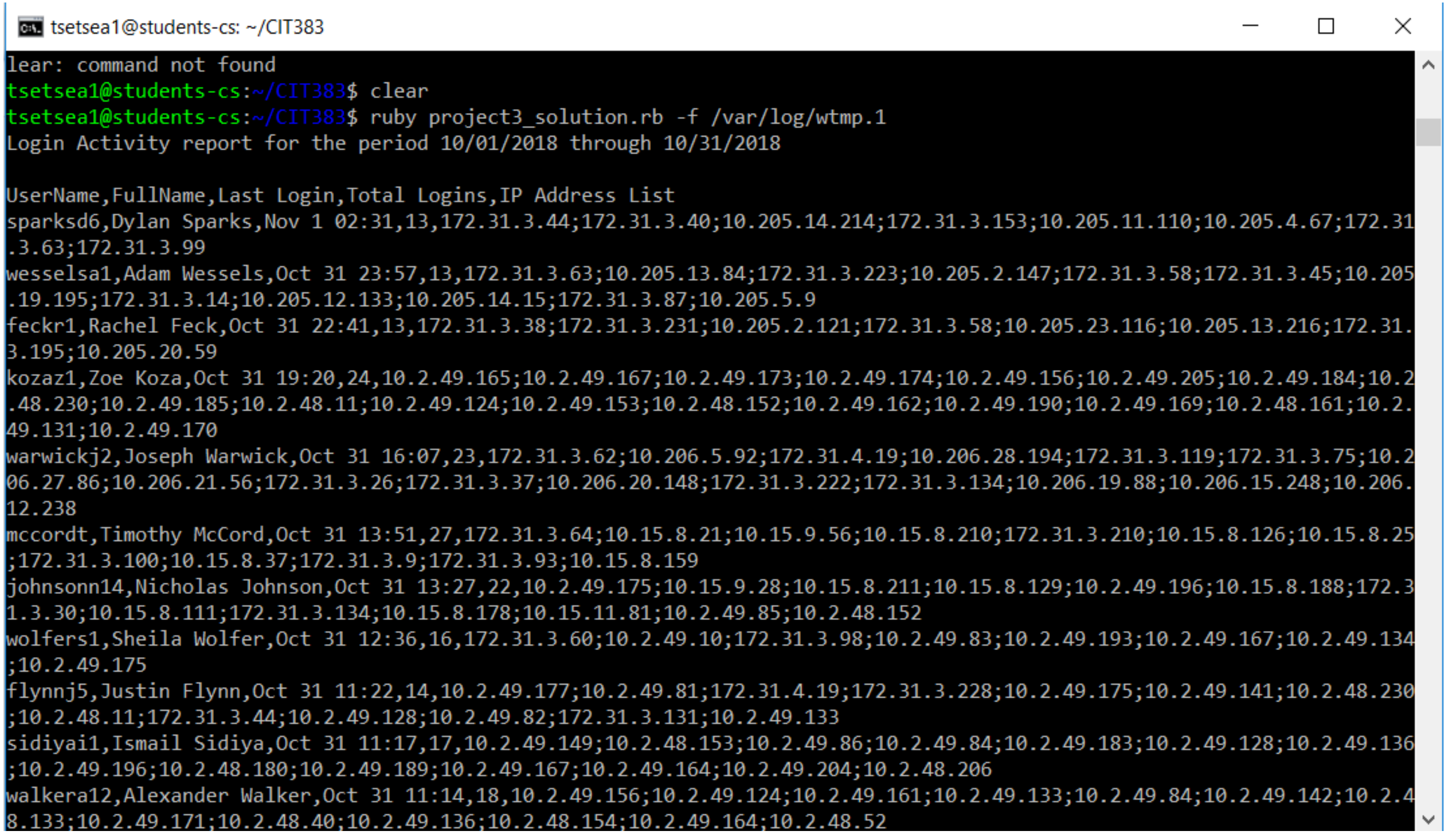
Run using –i option



```
tsetsea1@students-cs:~/CIT383$ clear
tsetsea1@students-cs:~/CIT383$ clear
tsetsea1@students-cs:~/CIT383$ ruby project3_solution.rb -i
Login Activity report for the period 11/01/2018 through 11/30/2018

UserName,FullName,Last Login,Total Logins,IP Address List
tsetsea1,Anthony Tsetse,Nov 26 23:59,28,172.31.4.236;10.15.8.200;172.31.3.113;172.31.4.212;10.206.21.159;10.15.27.116;17
2.31.3.44;172.31.3.147;172.31.4.22;172.31.3.158
kozaz1,Zoe Koza,Nov 26 22:45,17,10.2.49.209;10.2.49.185;10.2.49.190;10.2.49.81;10.2.48.180;10.2.49.143;10.2.49.188;10.2.
49.123;10.2.49.5;10.2.49.174;10.2.48.131;10.2.49.177;10.2.49.165;10.2.48.11
futscherj2,Jay Futscher,Nov 26 21:22,6,10.205.24.18;10.206.3.103;172.31.3.176;10.206.15.10
wrightr9,Rachel Wright,Nov 26 20:24,6,10.205.23.129;172.31.3.212;172.31.3.138;10.205.1.39
detellemd1,Douglas Detellem,Nov 26 19:48,15,10.2.49.5;10.2.48.161;10.2.49.185;10.2.48.120;172.31.3.60
thorpz1,Zachary Thorp,Nov 26 19:44,13,10.2.49.164;172.31.3.89;172.31.3.101;172.31.4.187;10.2.48.152;10.205.7.1;172.31.3.
80;10.2.49.166;172.31.3.102;172.31.3.114;172.31.3.85
damesm1,Michael Dames,Nov 26 19:40,7,10.2.49.196;10.15.8.144;172.31.3.174;172.31.3.154;172.31.3.135;172.31.3.146;172.31.
3.88
kwanp1,Pak Kwan,Nov 26 19:07,4,10.15.8.200
wolfers1,Sheila Wolfer,Nov 26 18:47,20,10.2.49.175;10.2.49.142;172.31.3.70;10.2.49.184;10.2.50.82;10.2.49.132;10.2.48.13
1;10.2.48.42;10.2.48.152;10.2.49.170;10.2.49.83
odoya1,Ashtin Odoy,Nov 26 18:36,2,172.31.3.130;10.205.7.61
schulkensc1,Christopher Schulkens,Nov 26 18:30,10,10.2.49.128;10.2.49.173;10.2.48.42;10.2.49.150;10.2.48.61;172.31.3.65;
172.31.3.157;172.31.3.111;10.15.9.45
streetb1,Brian Street,Nov 26 18:29,3,10.15.9.46
dupontb1,Bronson Dupont,Nov 26 18:27,6,10.2.49.86;10.2.49.83;10.2.49.189;10.2.48.161
wellsk11,Kenton Wells,Nov 26 18:26,18,10.205.25.4;172.31.3.126;172.31.3.105;10.205.16.75;10.205.0.239;172.31.3.198;172.3
1.3.145;172.31.3.149;10.205.22.144
stockl1,Lisa Stock,Nov 26 18:09,12,10.15.8.117;10.2.48.157;10.15.8.70;10.2.49.123;10.15.8.55;10.2.49.194
petersb1,Brittany Peters,Nov 26 17:40,20,10.2.48.40;10.2.49.141;10.2.49.184;10.2.49.132;10.2.48.131;10.2.49.151;10.2.48.
79;10.2.49.171;10.2.48.154;10.2.48.133;10.2.49.150
```

Run using –f option to have last command open a specific file



```
lear: command not found
tsetsea1@students-cs:~/CIT383$ clear
tsetsea1@students-cs:~/CIT383$ ruby project3_solution.rb -f /var/log/wtmp.1
Login Activity report for the period 10/01/2018 through 10/31/2018

UserName,FullName,Last Login,Total Logins,IP Address List
sparksd6,Dylan Sparks,Nov 1 02:31,13,172.31.3.44;172.31.3.40;10.205.14.214;172.31.3.153;10.205.11.110;10.205.4.67;172.31
.3.63;172.31.3.99
wesselsa1,Adam Wessels,Oct 31 23:57,13,172.31.3.63;10.205.13.84;172.31.3.223;10.205.2.147;172.31.3.58;172.31.3.45;10.205
.19.195;172.31.3.14;10.205.12.133;10.205.14.15;172.31.3.87;10.205.5.9
feckr1,Rachel Feck,Oct 31 22:41,13,172.31.3.38;172.31.3.231;10.205.2.121;172.31.3.58;10.205.23.116;10.205.13.216;172.31.
3.195;10.205.20.59
kozaz1,Zoe Koza,Oct 31 19:20,24,10.2.49.165;10.2.49.167;10.2.49.173;10.2.49.174;10.2.49.156;10.2.49.205;10.2.49.184;10.2
.48.230;10.2.49.185;10.2.48.11;10.2.49.124;10.2.49.153;10.2.48.152;10.2.49.162;10.2.49.190;10.2.49.169;10.2.48.161;10.2.
49.131;10.2.49.170
warwickj2,Joseph Warwick,Oct 31 16:07,23,172.31.3.62;10.206.5.92;172.31.4.19;10.206.28.194;172.31.3.119;172.31.3.75;10.2
06.27.86;10.206.21.56;172.31.3.26;172.31.3.37;10.206.20.148;172.31.3.222;172.31.3.134;10.206.19.88;10.206.15.248;10.206.
12.238
mccordt,Timothy McCord,Oct 31 13:51,27,172.31.3.64;10.15.8.21;10.15.9.56;10.15.8.210;172.31.3.210;10.15.8.126;10.15.8.25
;172.31.3.100;10.15.8.37;172.31.3.9;172.31.3.93;10.15.8.159
johnsonn14,Nicholas Johnson,Oct 31 13:27,22,10.2.49.175;10.15.9.28;10.15.8.211;10.15.8.129;10.2.49.196;10.15.8.188;172.3
1.3.30;10.15.8.111;172.31.3.134;10.15.8.178;10.15.11.81;10.2.49.85;10.2.48.152
wolfers1,Sheila Wolfer,Oct 31 12:36,16,172.31.3.60;10.2.49.10;172.31.3.98;10.2.49.83;10.2.49.193;10.2.49.167;10.2.49.134
;10.2.49.175
flynnj5,Justin Flynn,Oct 31 11:22,14,10.2.49.177;10.2.49.81;172.31.4.19;172.31.3.228;10.2.49.175;10.2.49.141;10.2.48.230
;10.2.48.11;172.31.3.44;10.2.49.128;10.2.49.82;172.31.3.131;10.2.49.133
sidiyai1,Ismail Sidiya,Oct 31 11:17,17,10.2.49.149;10.2.48.153;10.2.49.86;10.2.49.84;10.2.49.183;10.2.49.128;10.2.49.136
;10.2.49.196;10.2.48.180;10.2.49.189;10.2.49.167;10.2.49.164;10.2.49.204;10.2.48.206
walkera12,Alexander Walker,Oct 31 11:14,18,10.2.49.156;10.2.49.124;10.2.49.161;10.2.49.133;10.2.49.84;10.2.49.142;10.2.4
8.133;10.2.49.171;10.2.48.40;10.2.49.136;10.2.48.154;10.2.49.164;10.2.48.52
```