Reader/Writer Python Script

inputfile = open('log.xml','r')  
outputfile = open('output.xml','w')  
  
numevents = 0  
  
  
for line in inputfile:  
      
    do other stuff  
  
    outputfile.write(line)  
      
    numevents++  
      
f.close()  
g.close()

Stage 1

Stage 1 – Analysis You Can See

You may use any tools you would like to do the analysis. I would recommend trying Microsoft Excel as well as Notepad++ (not Windows Notepad).  Consider using Tableau for advanced visualizations. Y

Part A

Review the supplied Windows Security Log.  Report some basic statistics about it to include:

* When is the first event? **When systemtime was 2011-04-16T08:58:35.484375000Z**
* When is the last event? **When systemtime was 2011-04-16T15:07:53.890625000Z**
* Comment on the time stamps in the log file. What time zone are they in?
* How many total events are reported? **19702 events**

Part B

Focus on the events for EventID 4624 only and report the following:

* How many different users (as opposed to computers) log on to the network? **2405 users**
* Which users log on more times than other users? **David.spade**
* Make a frequency chart of when this user logs in

Part C

Focus on the events for EventID 4625 only and report the following**:(No event with eventid 4625 in the log file)**

* How many times is this EventID reported?
* Describe each of these events focusing on the user accounts and computers that were involved.
* What do you think should be done to solve this issue?

Part D

Reporting of tools you used

* Report which software tools you used.

-Visual studio code

-Python programming language

-Beautifulsoup(python library)

* Identify the methods you used to find the information

**I used a python program**

* Report and functions, scripts or semi-automated methods you applied in the tools

**1)First i opened the file using python then parsed it using Beautifulsoup**

**2)Then i used Beautifulsoup find\_all() function to get individual event from the file then stored the events in a list**

**3)Looping through the list i accessed the events one by one,then used Beautifulsoup find() function to get any tag inside the event**

**4)Finally i used .get\_text() function to get the text inside the tag**

Stage 2

Stage 2 – Programming

Using a programming language of your choice, write an application to scan through the supplied data file and generate output about each Event ID Type.  You may choose Java, Python, or a combination of Bash and Linux commands like grep, awk, and sed.  These are potentially powerful commands that can be scripted and linked together with piping.  See this tutorial: [https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site." HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site." HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site." HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf" HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site." HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site." HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site."  HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site." HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site." HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site." HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf" HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site." HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site." HYPERLINK "https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd\_year\_Comp\_Lab/guides/grep\_awk\_sed.pdf%22site."site.](https://www-users.york.ac.uk/~mijp1/teaching/2nd_year_Comp_Lab/guides/grep_awk_sed.pdf%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd_year_Comp_Lab/guides/grep_awk_sed.pdf%22%A0%20HYPERLINK%20%22https://www-users.york.ac.uk/~mijp1/teaching/2nd_year_Comp_Lab/guides/grep_awk_sed.pdf%22site.)or one of many others out on the internet.

Part A

Your program should read the file as input and write an output file.  To start, you probably want to create a file reader/writer that simply duplicates the existing file line-by-line.

Part B

Modify your program to only duplicate lines into your output file that are associated with a specified EventID.  Notice that the input file has multiple lines per “event” and the EventID is \*NOT\* on the first line.  Your program can either accept as input from the keyboard which EventID to generate the file for, or you can hard code that into your program as a static variable.

Generate an output file for the Event ID 4624(**file 'events with id 4624.xml**')

Part C

Modify your program to generate a count of the number of times that the event ID occurs.  Run your program and generate and output file for Event ID 4625.

Part D

Modify your program to report the number of times that the given event ID occurs over time.  Your program should report the number of times each eventID occurs during each hour.  Your output should looks like the following:

2011-04-15T14   20  
2011-04-15T15   8  
2011-04-15T16   3  
2011-04-15T17   29  
Etc.

Generate the output for Event ID 4624 (**file 'eventid(4624).xml'**)