

Digital Forensics - Lab 2

Class No :	CH2021221000516	Slot :	L49 + L50
Course Code :	CSE4004	Faculty Name :	

Aadhitya Swarnesh



- 12 August 2021

Question 1 :

Download and install Microsoft's Log Parser tool for the Windows environment from Microsoft's Web Site.

Read the examples and take screenshots by running three different commands that work

For this experiment, I have used a windows 7 installed in a virtual machine. I have installed the required log parser version 2.2 from the Microsoft website. Using this I have obtained the outputs as shown below. I have first navigated to the folder where the log parser software is present, and then we execute the commands specified below.

I have tried a few commands and have tried different versions of the same too, I have explained each and have shown the output of each.

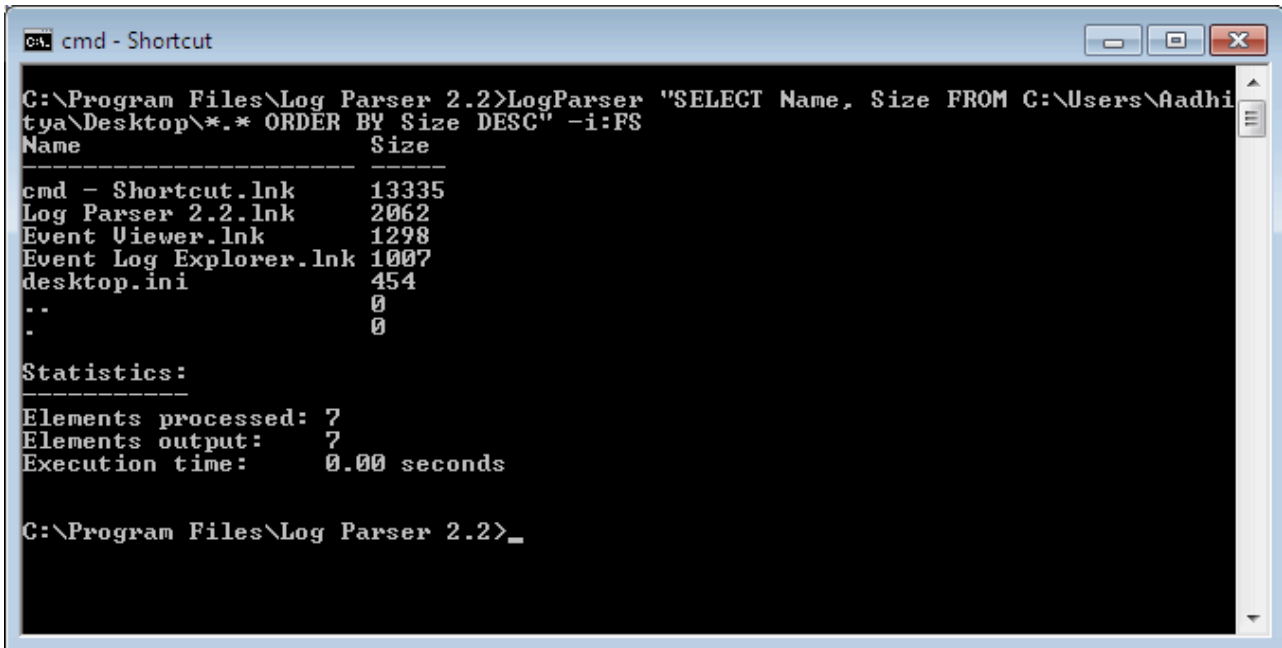
A. Display the contents of the Desktop folder

In order to do this we, design the query as follows :

*LogParser "SELECT Name, Size FROM C:\Users\UserName\Desktop\ *.* ORDER BY
Size DESC" -i:FS*



We have displayed the name and size of the contents of the desktop folder, I have also ordered the files by their size in descending order. The output I have received when executed is as follows :



```
C:\Program Files\Log Parser 2.2>LogParser "SELECT Name, Size FROM C:\Users\Aadhitya\Desktop\*. * ORDER BY Size DESC" -i:FS
Name                                     Size
-----
cmd - Shortcut.lnk                      13335
Log Parser 2.2.lnk                      2062
Event Viewer.lnk                        1298
Event Log Explorer.lnk                  1007
desktop.ini                             454
..                                       0
.                                       0

Statistics:
-----
Elements processed: 7
Elements output: 7
Execution time: 0.00 seconds

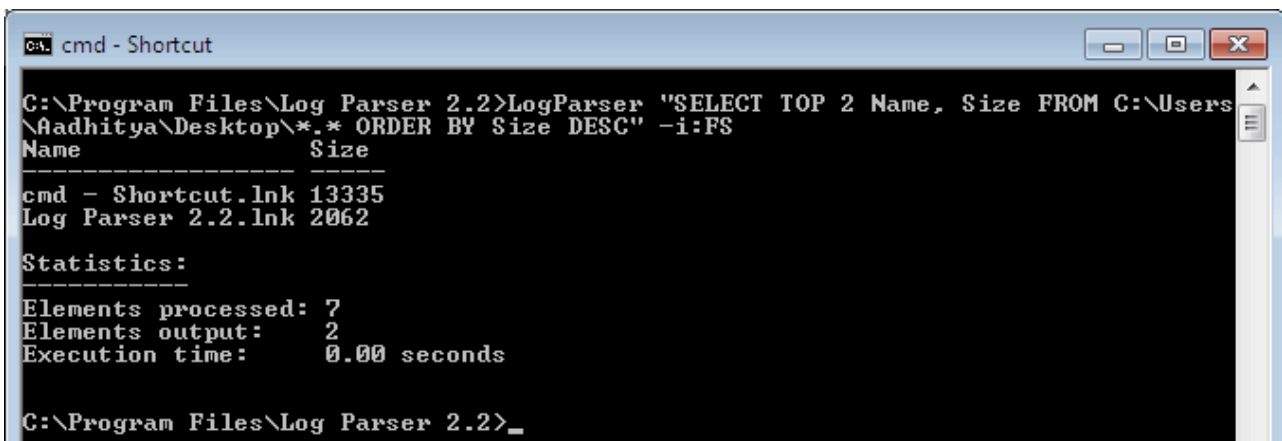
C:\Program Files\Log Parser 2.2>_
```

B. Display the 2 largest files in the Desktop folder

In order to do this we, design the query as follows :

LogParser "SELECT TOP 2 Name, Size FROM C:\Users\UserName\Desktop. *
ORDER BY Size DESC" -i:FS*

We have displayed the name and size of the two largest files in the desktop folder, I have also ordered the files by their size in descending order. The output I have received when executed is as follows :



```
C:\Program Files\Log Parser 2.2>LogParser "SELECT TOP 2 Name, Size FROM C:\Users\Aadhitya\Desktop\*. * ORDER BY Size DESC" -i:FS
Name                                     Size
-----
cmd - Shortcut.lnk                      13335
Log Parser 2.2.lnk                      2062

Statistics:
-----
Elements processed: 7
Elements output: 2
Execution time: 0.00 seconds

C:\Program Files\Log Parser 2.2>_
```

C. Display all the currently listening Network ports

In order to create a log parser query for this, we redirect the output of the “**netstat**” command to the log parser query.

The “**netstat**” command is used to display all the open network ports. An example output of this command is as follows :

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Aadhitya>netstat -a

Active Connections

Proto Local Address Foreign Address State
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:49159 TIME_WAIT
TCP Aadhitya-PC:49160 ESTABLISHED
TCP Aadhitya-PC:49158 TIME_WAIT
TCP Aadhitya-PC:49161 TIME_WAIT
TCP Aadhitya-PC:icslap ESTABLISHED
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
TCP Aadhitya-PC:0 LISTENING
```

We can notice that the state denotes the state of the port, we will use this in our query, we will divert the output into the log parser using the pipeline command. The final log parser query is as follows :

```
netstat -a | LogParser -i:TSV "SELECT * FROM STDIN WHERE State='LISTENING'"
-iSeperator:space -nSep:2 -fixedSep:OFF -nSkipLines:2
```

```

cmd - Shortcut
C:\Program Files\Log Parser 2.2>netstat -a | LogParser -i:TSU "SELECT * FROM STDIN WHERE State='LISTENING'" -iSeparator:space -nSep:2 -fixedSep:OFF -nSkipLines:2

```

Filename	RowNumber	Proto	Local Address	Foreign Address	State
STDIN	5	TCP		Aadhitya-PC:0	LISTENING
STDIN	6	TCP		Aadhitya-PC:0	LISTENING
STDIN	7	TCP		Aadhitya-PC:0	LISTENING
STDIN	8	TCP		Aadhitya-PC:0	LISTENING
STDIN	9	TCP		Aadhitya-PC:0	LISTENING
STDIN	10	TCP		Aadhitya-PC:0	LISTENING
STDIN	11	TCP		Aadhitya-PC:0	LISTENING
STDIN	12	TCP		Aadhitya-PC:0	LISTENING
STDIN	13	TCP		Aadhitya-PC:0	LISTENING
STDIN	14	TCP		Aadhitya-PC:0	LISTENING

Press a key...

Filename	RowNumber	Proto	Local Address	Foreign Address	State
STDIN	15	TCP		Aadhitya-PC:0	LISTENING
STDIN	16	TCP		Aadhitya-PC:0	LISTENING
STDIN	17	TCP		Aadhitya-PC:0	LISTENING
STDIN	18	TCP		Aadhitya-PC:0	LISTENING
STDIN	19	TCP		Aadhitya-PC:0	LISTENING
STDIN	20	TCP		Aadhitya-PC:0	LISTENING
STDIN	21	TCP		Aadhitya-PC:0	LISTENING
STDIN	22	TCP		Aadhitya-PC:0	LISTENING
STDIN	23	TCP		Aadhitya-PC:0	LISTENING
STDIN	24	TCP		Aadhitya-PC:0	LISTENING

Press a key...

Filename	RowNumber	Proto	Local Address	Foreign Address	State
STDIN	25	TCP		Aadhitya-PC:0	LISTENING
STDIN	26	TCP		Aadhitya-PC:0	LISTENING
STDIN	27	TCP		Aadhitya-PC:0	LISTENING
STDIN	28	TCP		Aadhitya-PC:0	LISTENING

Statistics:

```

Elements processed: 56
Elements output: 24
Execution time: 2.13 seconds

```

```

cmd - Shortcut
C:\Program Files\Log Parser 2.2>netstat -a | LogParser -i:TSU "SELECT [Local Address] FROM STDIN WHERE State='LISTENING'" -iSeparator:space -nSep:2 -fixedSep:OFF -nSkipLines:2

```

Local Address

Press a key...

Local Address

Press a key...

Local Address

Statistics:

```

Elements processed: 56
Elements output: 24
Execution time: 3.21 seconds

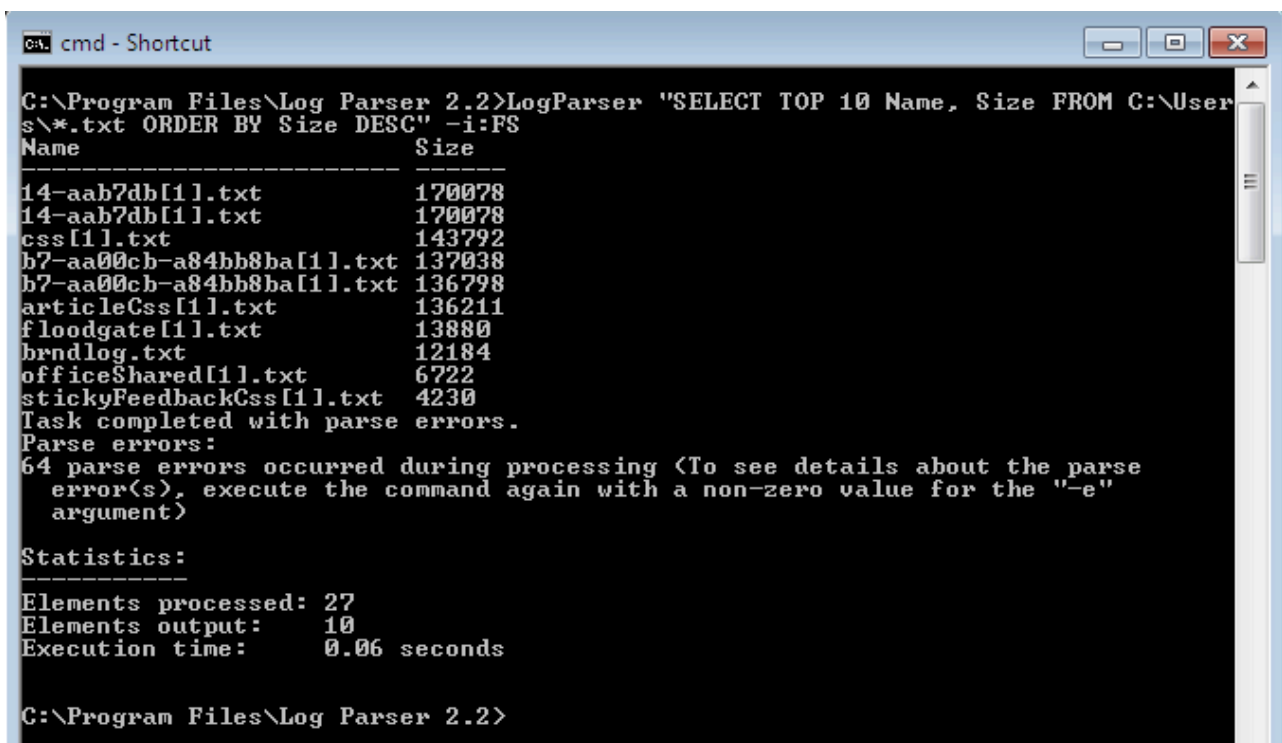
```

D. Display the 10 largest text files from the users folder in windows C drive

In order to do this we, design the query as follows :

LogParser "SELECT TOP 10 Name, Size FROM C:\Users.txt ORDER BY Size DESC" -i:FS*

We have displayed the name and size of the ten largest text files in the Users folder, I have also ordered the files by their size in descending order. Notice that text file have an extension of ".txt", we have used this property to filter out the text files. The output I have received when executed is as follows :



```
cmd - Shortcut
C:\Program Files\Log Parser 2.2>LogParser "SELECT TOP 10 Name, Size FROM C:\User
s\*.txt ORDER BY Size DESC" -i:FS
Name                               Size
-----
14-aab7db[1].txt                   170078
14-aab7db[1].txt                   170078
css[1].txt                         143792
b7-aa00cb-a84bb8ba[1].txt         137038
b7-aa00cb-a84bb8ba[1].txt         136798
articleCss[1].txt                 136211
floodgate[1].txt                  13880
hrndlog.txt                       12184
officeShared[1].txt               6722
stickyFeedbackCss[1].txt          4230
Task completed with parse errors.
Parse errors:
64 parse errors occurred during processing (To see details about the parse
error(s), execute the command again with a non-zero value for the "-e"
argument)

Statistics:
-----
Elements processed: 27
Elements output:    10
Execution time:     0.06 seconds

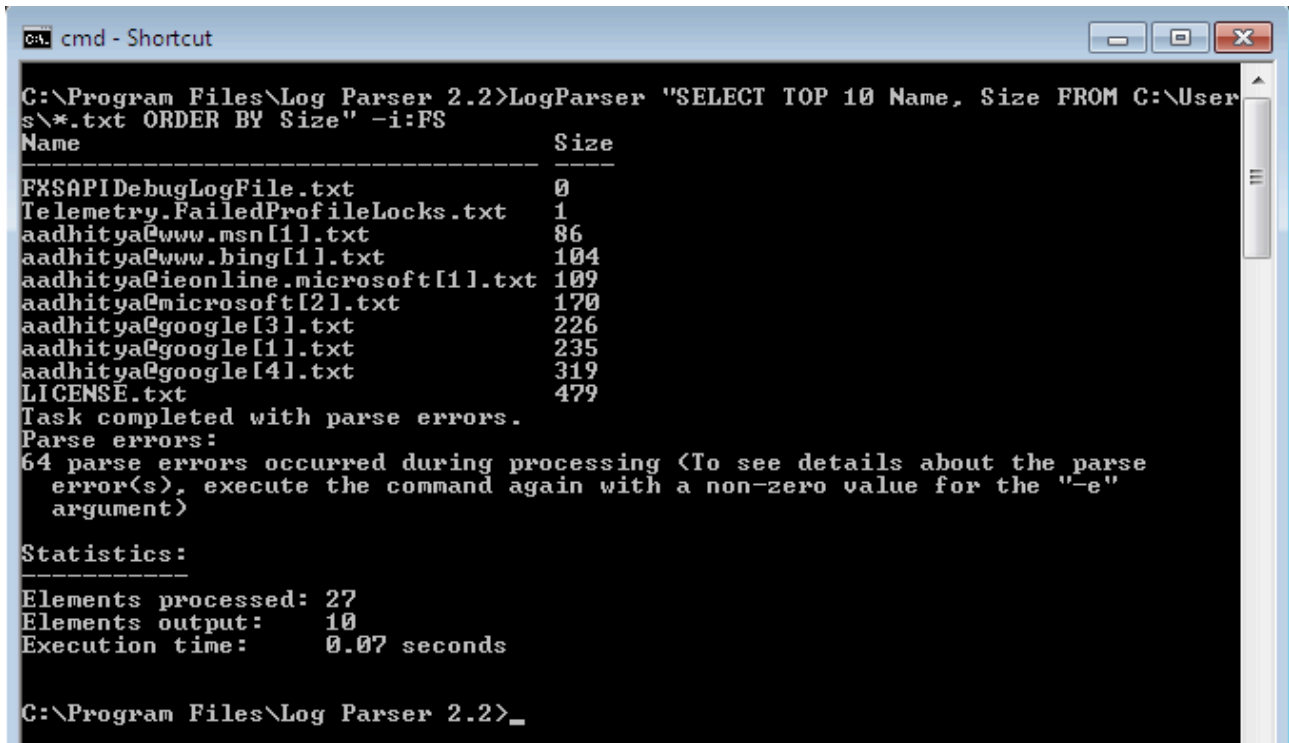
C:\Program Files\Log Parser 2.2>
```

E. Display the 10 smallest text files from the users folder in windows C drive

In order to do this we, design the query as follows :

LogParser "SELECT TOP 10 Name, Size FROM C:\Users.txt ORDER BY Size" -i:FS*

We have displayed the name and size of the ten smallest text files in the Users folder, I have also ordered the files by their size in descending order. Notice that text file have an extension of “.txt”, we have used this property to filter out the text files. The output I have received when executed is as follows :



```
cmd - Shortcut
C:\Program Files\Log Parser 2.2>LogParser "SELECT TOP 10 Name, Size FROM C:\User
s\*.txt ORDER BY Size" -i:FS
Name                                     Size
-----
FXSAPIDebugLogFile.txt                  0
Telemetry.FailedProfileLocks.txt        1
aadhitya@www.msn[1].txt                  86
aadhitya@www.bing[1].txt                 104
aadhitya@ieonline.microsoft[1].txt      109
aadhitya@microsoft[2].txt                170
aadhitya@google[3].txt                   226
aadhitya@google[1].txt                   235
aadhitya@google[4].txt                   319
LICENSE.txt                             479
Task completed with parse errors.
Parse errors:
64 parse errors occurred during processing (To see details about the parse
error(s), execute the command again with a non-zero value for the "-e"
argument)

Statistics:
-----
Elements processed: 27
Elements output:    10
Execution time:     0.07 seconds

C:\Program Files\Log Parser 2.2>_
```

CONCLUSION

We have in this experiment, performed many forensic analysis on the hard disk folders using Microsoft's Log Parser Tool, like knowing the top 10 largest or smallest files, or to use the log parser tool for higher purposes by redirecting the output of other commands to this, like finding the network ports with a particular status, etc.