

CSE 4004

Digital Forensics

**Lab
Session 2**

TOPIC: File analysis tool - log parser

Name: Makesh Srinivasan

Registration number: 19BCE1717

Slot: L49 + L50

Date: 26-Aug-2021-Thursday

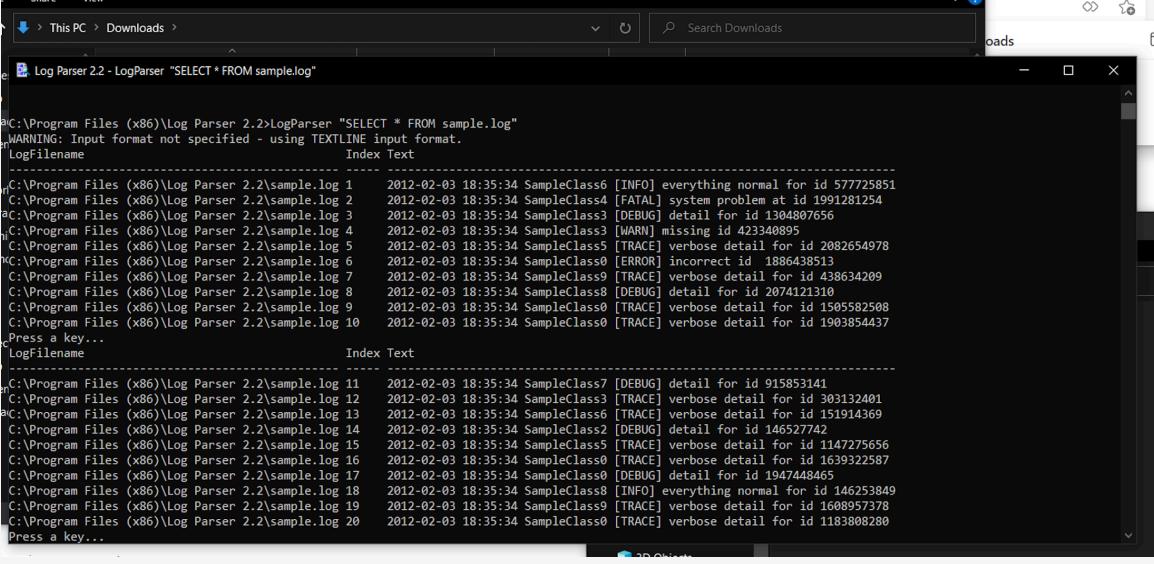
Faculty: Prof. Nagaraj

AIM: To run 3 example commands on Microsoft Log Parser and observe the results

INSTRUCTIONS:

Download and install Microsoft's Log Parser tool for the Windows environment from Microsoft's Web Site: <https://www.microsoft.com/en-in/download/details.aspx?id=24659> Read the examples and take screenshots by running three different commands that work.

OBSERVATION:

1	LogParser "SELECT * FROM sample.log"
	 A screenshot of the Log Parser 2.2 application window. The title bar says "Log Parser 2.2 - LogParser "SELECT * FROM sample.log"". The main area shows log entries from "sample.log" files. The first entry is: "C:\Program Files (x86)\Log Parser 2.2\sample.log 1 2012-02-03 18:35:34 SampleClass6 [INFO] everything normal for id 577725851". There are many other entries with similar patterns, indicating various log levels (INFO, DEBUG, TRACE, ERROR, FATAL) and timestamps. The bottom of the window has a message "Press a key..." and a "Logfilename" dropdown menu with options "Index" and "Text".

- 2 LogParser "SELECT Text as LineFromFile FROM sample.log"

```
Gmail Search mail

Log Parser 2.2

Elements processed: 231
Elements output: 230
Execution time: 85.14 seconds (00:01:25.14)

C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT Text as LineFromFile FROM sample.log"
WARNING: Input format not specified - using TEXTLINE input format.
LineFromFile
-----
2012-02-03 18:35:34 SampleClass6 [INFO] everything normal for id 577725851
2012-02-03 18:35:34 SampleClass4 [FATAL] system problem at id 1991281254
2012-02-03 18:35:34 SampleClass3 [DEBUG] detail for id 1304807656
2012-02-03 18:35:34 SampleClass3 [WARN] missing id 423340895
2012-02-03 18:35:34 SampleClass5 [TRACE] verbose detail for id 2082654978
2012-02-03 18:35:34 SampleClass8 [ERROR] incorrect id 1886438513
2012-02-03 18:35:34 SampleClass9 [TRACE] verbose detail for id 438634209
2012-02-03 18:35:34 SampleClass8 [DEBUG] detail for id 2074121310
2012-02-03 18:35:34 SampleClass0 [TRACE] verbose detail for id 1505582508
2012-02-03 18:35:34 SampleClass0 [TRACE] verbose detail for id 1903854437
Press a key...
Task aborted by user.

Statistics:
-----
Elements processed: 31
Elements output: 30
Execution time: 5.82 seconds

C:\Program Files (x86)\Log Parser 2.2>
```

- 3 LogParser "SELECT Top 10 * FROM C:\19bce1717*.* ORDER BY Size DESC" -i:FS

```
File Log Parser 2.2

C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT Top 10 FROM C:\19bcel171\*.* ORDER BY Size DESC" -i:FS
Error: Syntax Error: <from-clause>: expecting FROM keyword instead of token 'C:\19bcel171\*.*'

C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT Top 10 * FROM C:\19bcel171\*.* ORDER BY Size DESC" -i:FS
Path          Name
en           Attributes creationTime      LastAccessTime     LastWriteTime    FileVersion ProductVersion InternalName ProductName CompanyName LegalCopyright LegalTradem
s arks          SpecialBuild Comments FileDescription OriginalFilename
on

ra: C:\19bcel171\chemistry one shot revision on Basic concepts of chemistry-20210722_055011-Meeting Recording.mp4 Chemistry one shot revision on Basic concepts of chemistry-20210722_055011-Meeting Re
rcording.mp4 144452767 -A----- 2021-08-26 11:48:09.306 2021-08-26 11:48:09.497 2021-07-22 14:43:35.409 -
ra: C:\19bcel171\Empirical formula.mp4
10353978 -A----- 2021-08-26 11:48:09.113 2021-08-26 11:48:09.132 2021-07-28 08:36:48.987 -
ra: C:\19bcel171\Class-11-Physics-Part-1 (1).pdf
9439000 -A----- 2021-08-26 11:48:09.561 2021-08-26 11:48:09.576 2021-08-01 16:59:12.920 -
ra: C:\19bcel171\computer record.docx
3578070 -A----- 2021-08-26 11:48:09.672 2021-08-26 11:48:09.675 2021-08-17 13:15:36.908 -
ra: C:\19bcel171\chemistry 6th weekend submission.pdf
2460928 -A----- 2021-08-26 11:48:09.231 2021-08-26 11:48:09.239 2021-07-16 14:13:46.824 -
ra: C:\19bcel171\chemistry 3rd weekend submission somwya.pdf
2287104 -A----- 2021-08-26 11:48:09.162 2021-08-26 11:48:09.173 2021-06-25 13:16:21.91 -
ra: C:\19bcel171\chemistry somwya weekend submission.pdf
2089497 -A----- 2021-08-26 11:48:09.532 2021-08-26 11:48:09.540 2021-06-11 16:55:48.930 -
ra: C:\19bcel171\computer input output devices somwya.pdf
1876758 -A----- 2021-08-26 11:48:09.590 2021-08-26 11:48:09.599 2021-06-07 16:13:03.183 -
ra: C:\19bcel171\computer input output devices somwyaari.pdf
1876758 -A----- 2021-08-26 11:48:09.611 2021-08-26 11:48:09.619 2021-06-07 16:27:42.462 -
ra: C:\19bcel171\chemistry midterm somwya.pdf
1621287 -A----- 2021-08-26 11:48:09.294 2021-08-26 11:48:09.302 2021-08-09 16:53:18.561 -
ra: Statistics:
Elements processed: 19
Elements output: 10
Execution time: 0.23 seconds
```

RESULTS:

As shown above, 4 commands were executed on LogParser on a windows 10 operating system and the outputs are attached in the section above.