

**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

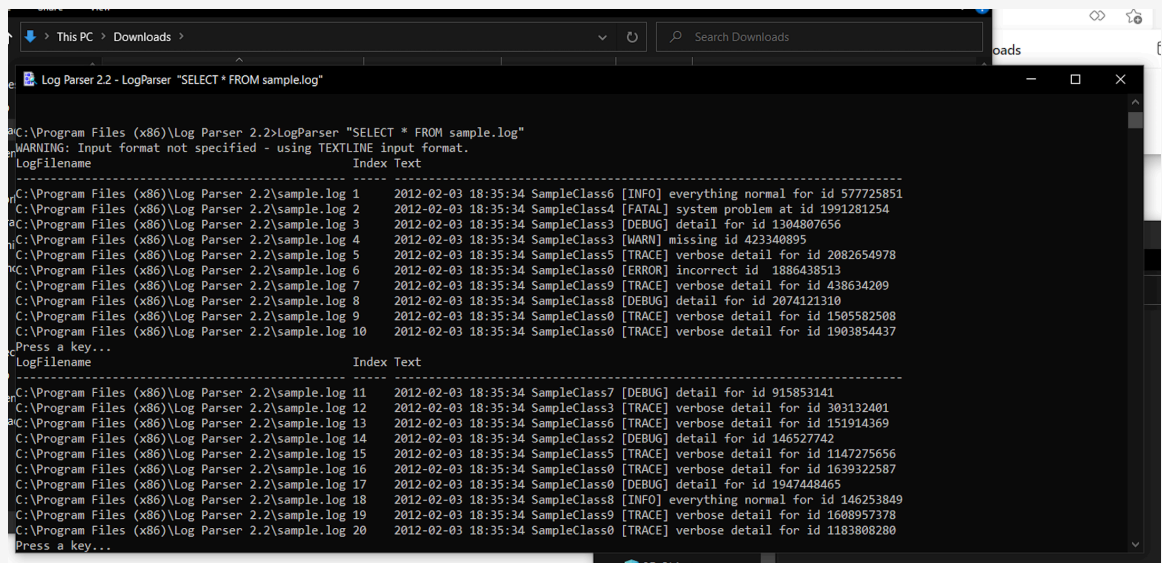
**AIM:** To run 3 example commands on Microsoft Log Parser and observe the results

## 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"



```
C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT * FROM sample.log"
WARNING: Input format not specified - using TEXTLINE input format.
LogFilename                               Index Text
-----
C:\Program Files (x86)\Log Parser 2.2\sample.log 1 2012-02-03 18:35:34 SampleClass6 [INFO] everything normal for id 577725851
C:\Program Files (x86)\Log Parser 2.2\sample.log 2 2012-02-03 18:35:34 SampleClass4 [FATAL] system problem at id 1991281254
C:\Program Files (x86)\Log Parser 2.2\sample.log 3 2012-02-03 18:35:34 SampleClass3 [DEBUG] detail for id 1304807656
C:\Program Files (x86)\Log Parser 2.2\sample.log 4 2012-02-03 18:35:34 SampleClass3 [WARN] missing id 423340895
C:\Program Files (x86)\Log Parser 2.2\sample.log 5 2012-02-03 18:35:34 SampleClass5 [TRACE] verbose detail for id 2082654978
C:\Program Files (x86)\Log Parser 2.2\sample.log 6 2012-02-03 18:35:34 SampleClass0 [ERROR] incorrect id 1886438513
C:\Program Files (x86)\Log Parser 2.2\sample.log 7 2012-02-03 18:35:34 SampleClass9 [TRACE] verbose detail for id 438634209
C:\Program Files (x86)\Log Parser 2.2\sample.log 8 2012-02-03 18:35:34 SampleClass8 [DEBUG] detail for id 2074121310
C:\Program Files (x86)\Log Parser 2.2\sample.log 9 2012-02-03 18:35:34 SampleClass0 [TRACE] verbose detail for id 1505582508
C:\Program Files (x86)\Log Parser 2.2\sample.log 10 2012-02-03 18:35:34 SampleClass0 [TRACE] verbose detail for id 1903854437
Press a key...
LogFilename                               Index Text
-----
C:\Program Files (x86)\Log Parser 2.2\sample.log 11 2012-02-03 18:35:34 SampleClass7 [DEBUG] detail for id 915853141
C:\Program Files (x86)\Log Parser 2.2\sample.log 12 2012-02-03 18:35:34 SampleClass3 [TRACE] verbose detail for id 303132401
C:\Program Files (x86)\Log Parser 2.2\sample.log 13 2012-02-03 18:35:34 SampleClass6 [TRACE] verbose detail for id 151914369
C:\Program Files (x86)\Log Parser 2.2\sample.log 14 2012-02-03 18:35:34 SampleClass2 [DEBUG] detail for id 146527742
C:\Program Files (x86)\Log Parser 2.2\sample.log 15 2012-02-03 18:35:34 SampleClass5 [TRACE] verbose detail for id 1147275656
C:\Program Files (x86)\Log Parser 2.2\sample.log 16 2012-02-03 18:35:34 SampleClass0 [TRACE] verbose detail for id 1639322587
C:\Program Files (x86)\Log Parser 2.2\sample.log 17 2012-02-03 18:35:34 SampleClass0 [DEBUG] detail for id 1947448465
C:\Program Files (x86)\Log Parser 2.2\sample.log 18 2012-02-03 18:35:34 SampleClass8 [INFO] everything normal for id 146253849
C:\Program Files (x86)\Log Parser 2.2\sample.log 19 2012-02-03 18:35:34 SampleClass9 [TRACE] verbose detail for id 1608957378
C:\Program Files (x86)\Log Parser 2.2\sample.log 20 2012-02-03 18:35:34 SampleClass0 [TRACE] verbose detail for id 1183808280
Press a key...
```

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

```
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 SampleClass0 [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

```
Select Log Parser 2.2
C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT Top 10 * FROM C:\19bce1717\*. * ORDER BY Size DESC" -i:FS
Error: Syntax error: <from-clause>: expecting FROM keyword instead of token 'C:\19bce1717\*.*'

C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT Top 10 * FROM C:\19bce1717\*. * ORDER BY Size DESC" -i:FS
Path Size Attributes CreationTime LastAccessTime LastWriteTime FileVersion ProductVersion InternalName ProductName CompanyName LegalCopyright LegalTradem
-----
C:\19bce1717\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
C:\19bce1717\chemistry one shot revision on Basic concepts of chemistry-20210722_055011-Meeting Recording.mp4 144452767 -A----- 2021-08-26 11:48:09.306 2021-08-26 11:48:09.497 2021-07-22 14:43:35.409 -
C:\19bce1717\Emperical 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 -
C:\19bce1717\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 -
C:\19bce1717\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 -
C:\19bce1717\chemistry 6th weekend submission .pdf 2400328 -A----- 2021-08-26 11:48:09.231 2021-08-26 11:48:09.239 2021-07-16 14:13:46.824 -
C:\19bce1717\chemistry 3rd weekend submission sowmya.pdf 2207104 -A----- 2021-08-26 11:48:09.162 2021-08-26 11:48:09.173 2021-06-25 13:16:21.01 -
C:\19bce1717\chemistry sowmyaa weekend submission.pdf 2009497 -A----- 2021-08-26 11:48:09.532 2021-08-26 11:48:09.540 2021-06-11 16:55:48.930 -
C:\19bce1717\computer input output devices sowmyaa.pdf 1876758 -A----- 2021-08-26 11:48:09.590 2021-08-26 11:48:09.599 2021-06-07 16:13:03.183 -
C:\19bce1717\computer input output devices sowmyaasri.pdf 1876758 -A----- 2021-08-26 11:48:09.611 2021-08-26 11:48:09.619 2021-06-07 16:27:42.462 -
C:\19bce1717\chemistry midterm sowmya.pdf 1621287 -A----- 2021-08-26 11:48:09.294 2021-08-26 11:48:09.302 2021-08-09 16:53:18.561 -

Statistics:
-----
Elements processed: 19
Elements output: 10
Execution time: 0.23 seconds
```

#### 4 LogParser "SELECT Top 10 \* FROM C:\19bce1717\\*. \* ORDER BY Size ASC" -i:FS

```
C:\Program Files (x86)\Log Parser 2.2>LogParser "SELECT Top 10 * FROM C:\19bce1717\*. * ORDER BY Size ASC" -i:FS
Path Name Size Attributes CreationTime LastAccessTime LastWriteTime FileV
-----
C:\19bce1717\ 0 D----- 2021-08-26 11:47:33.490 2021-08-26 11:48:09.672 2021-08-26 11:48:09.672 -
C:\19bce1717\.. 0 D----- 2021-08-26 11:47:33.490 2021-08-26 11:48:09.672 2021-08-26 11:48:09.672 -
C:\19bce1717\chemistry hw atomic structure formula.pdf chemistry hw atomic structure formula.pdf 490678 -A----- 2021-08-26 11:48:09.275 2021-08-26 11:48:09.281 2021-07-15 11:31:39.870 -
C:\19bce1717\chemistry rules theory.pdf chemistry rules theory.pdf 728676 -A----- 2021-08-26 11:48:09.509 2021-08-26 11:48:09.516 2021-07-16 14:10:12.604 -
C:\19bce1717\chemistry 7th weekend submission .pdf chemistry 7th weekend submission .pdf 741840 -A----- 2021-08-26 11:48:09.252 2021-08-26 11:48:09.259 2021-07-23 12:25:00.814 -
C:\19bce1717\Computer midterm sowmya.pdf Computer midterm sowmya.pdf 1038872 -A----- 2021-08-26 11:48:09.650 2021-08-26 11:48:09.657 2021-08-11 16:59:18.592 -
C:\19bce1717\chemistry 4th weekend submission .pdf chemistry 4th weekend submission .pdf 1058685 -A----- 2021-08-26 11:48:09.188 2021-08-26 11:48:09.196 2021-07-09 12:10:39.483 -
C:\19bce1717\chemistry 5th weekend submission .pdf chemistry 5th weekend submission .pdf 1194614 -A----- 2021-08-26 11:48:09.208 2021-08-26 11:48:09.216 2021-07-09 12:17:57.492 -
C:\19bce1717\computer memory storage devices sowmya.pdf computer memory storage devices sowmya.pdf 1246758 -A----- 2021-08-26 11:48:09.631 2021-08-26 11:48:09.639 2021-06-07 16:18:16.511 -
C:\19bce1717\chemistry midterm sowmya.pdf chemistry midterm sowmya.pdf 1621287 -A----- 2021-08-26 11:48:09.294 2021-08-26 11:48:09.302 2021-08-09 16:53:18.561 -

Statistics:
-----
Elements processed: 19
Elements output: 10
Execution time: 0.02 seconds

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

### 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.