DIGITAL FORENSICS LAB

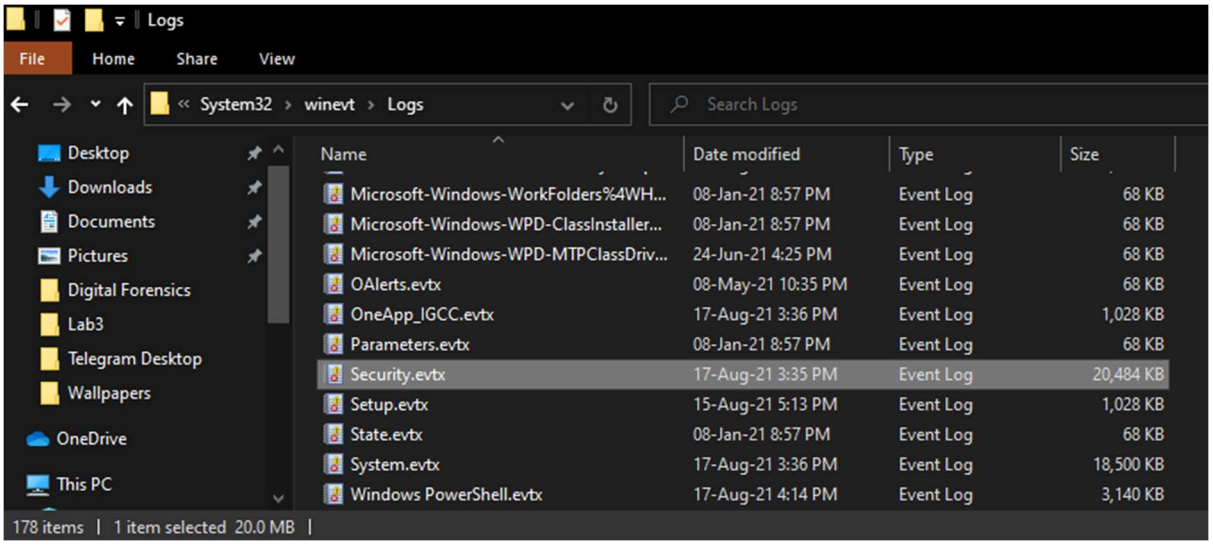
Exercise 2	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulgara
Date	17th August, 2021

AIM

Working with Windows Log Parser by executing commands, exploring switches and recording their outputs.

FILES USED

For this experiment, the Security.evtx file which contains the login/logoff and other security related events that happened in the system under investigation, which in this experiment is my personal laptop. Also, an XML file called 'books.xml' and a text file with comma separated values called 'Actors.txt' are used.



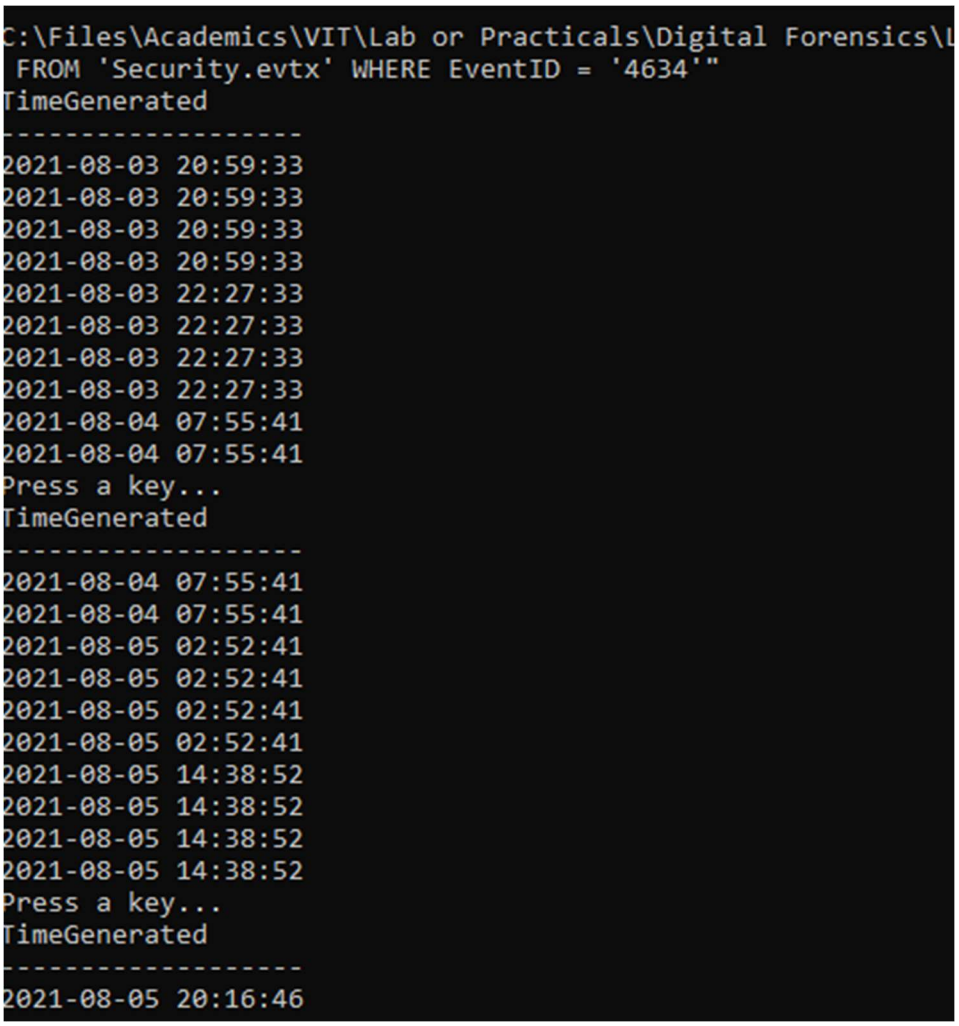
COMMANDS AND OUTPUTS

The tool used, LogParser2.2 is a CLI tool developed by a Microsoft employee to help query files such as logs using the familiar Structured Query Language. Each command begins with 'LogParser' (or to the path where it is installed if it is not added to the environment variable) followed by certain flags and the query. Some commands, their outputs and their interpretations are listed below.

COMMAND 1

```
LogParser.exe -stats:OFF -i:EVT "SELECT TimeGenerated FROM 'Security.evtx' WHERE EventID = '4634'"
```

OUTPUT



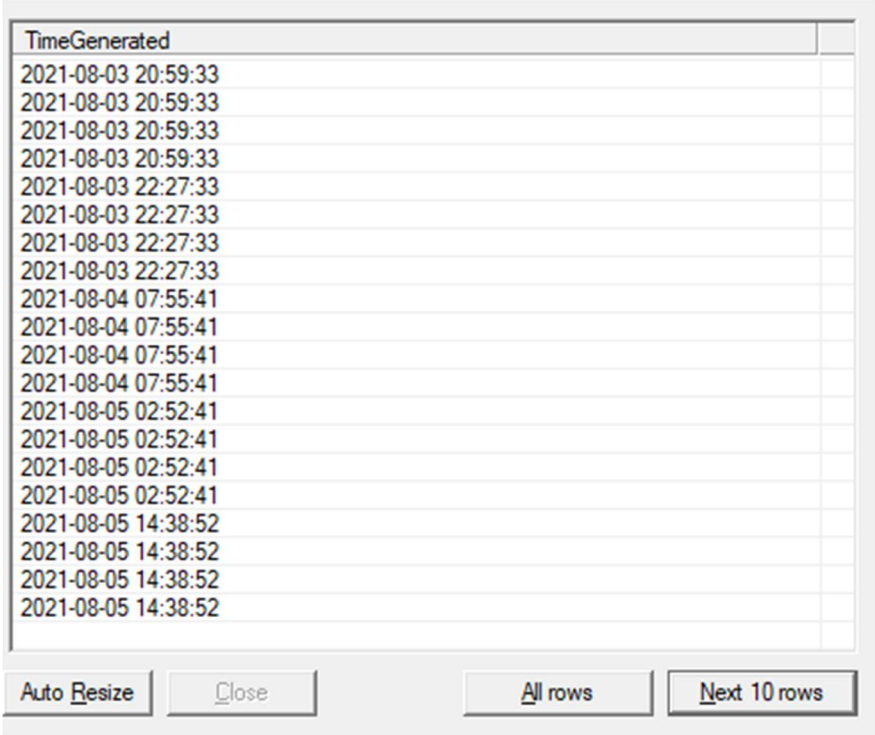
OBSERVATION

The command above is used to list the list of recoded time when an account was logged off. The '-i' switch is used to indicate the input format, which in this case is an EVT file. We parse the file to display the 'TimeGenerated' column values of those records whose 'EventID' is 4634, which indicates that an account was logged off.

COMMAND 2

```
LogParser.exe -stats:OFF -i:EVT "SELECT TimeGenerated FROM 'Security.evtx' WHERE EventID = '4634'" -o:datagrid
```

OUTPUT



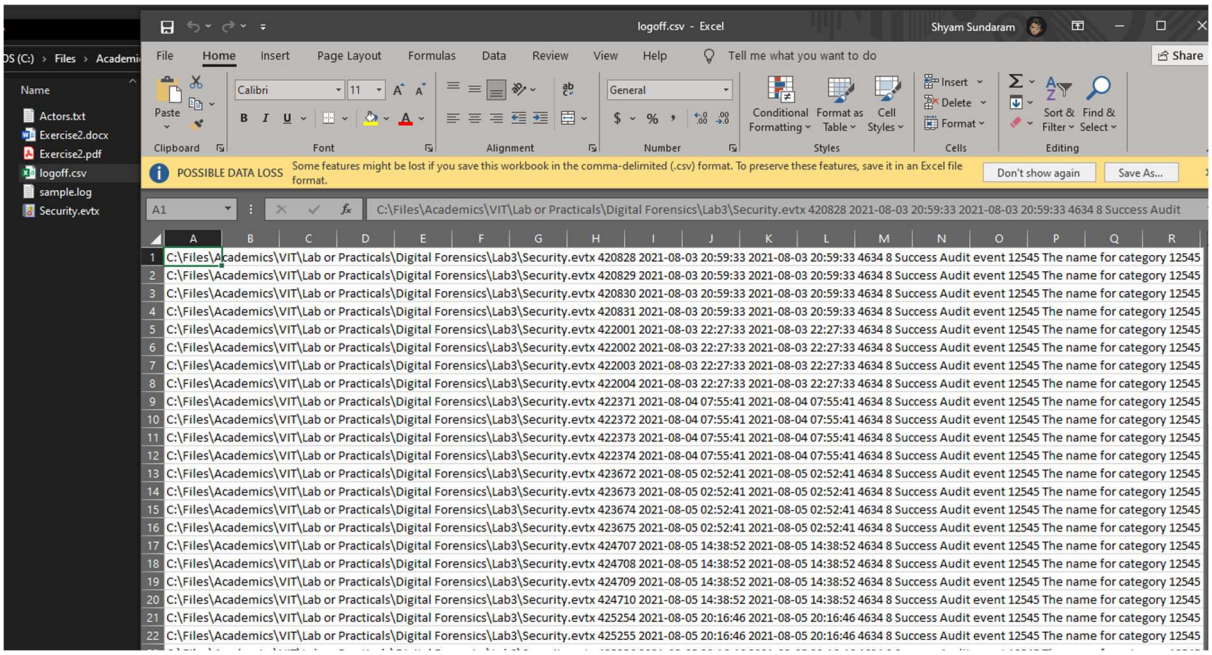
OBSERVATION

The command is used to display the same information as in the previous command, but with the help of 'datagrid', we get to see the output in a more readable format. The -o: switch is used to set the output type.

COMMAND 3

```
LogParser.exe -stats:OFF -i:EVT -q:ON "SELECT * FROM 'Security.evtx' WHERE EventID = '4634'" > logoff.csv
```

OUTPUT



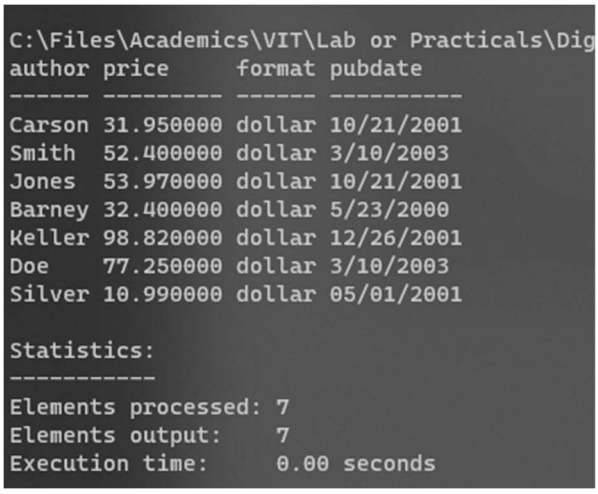
OBSERVATION

The command above is used to save the result or records returned by the query into a CSV file, here saved as logoff.csv. This CSV file contains all records whose EventID is 4634 which indicates that an account was logged off.

COMMAND 4

```
LogParser "SELECT * FROM books.xml" -fmode:Tree
```

OUTPUT



OBSERVATION

The command above is used to display the contents of an XML file called “books.xml”.

COMMAND 5

```
LogParser "SELECT Path, HASHMD5_FILE(Path) FROM sample.log" -i:FS -recurse:0
```

OUTPUT

```
C:\Files\Academics\VIT\Lab or Practicals\Digital Forensics\Lab3>LogParser "SELECT Path, HASHMD5_FILE(Path)
Path                                                                    HASHMD5_FILE(Path)
---------------------------------------------------------------------- --------------------------------
C:\Files\Academics\VIT\Lab or Practicals\Digital Forensics\Lab3\sample.log FB74068FA1EB9152479060D26590CD38

Statistics:
-----------
Elements processed: 1
Elements output:    1
Execution time:     0.01 seconds


C:\Files\Academics\VIT\Lab or Practicals\Digital Forensics\Lab3>
```

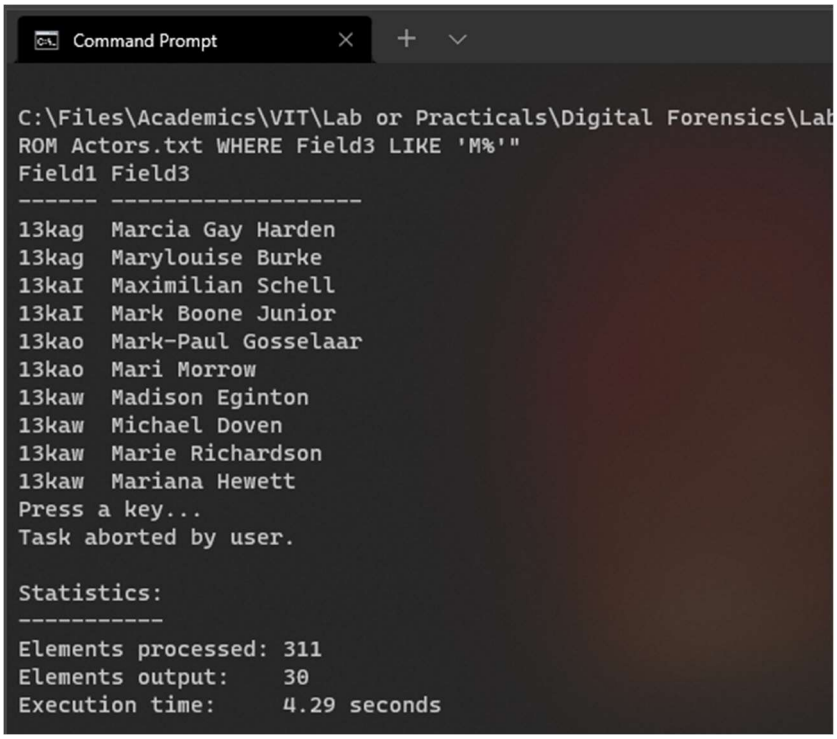
OBSERVATION

The command above returns the MD5 hash of the “sample.log” file. This can be used to verify whether or not a file has been tampered with. The ‘-i:FS’ switch is used to indicate that information on files and directories is being returned.

COMMAND 6

```
LogParser -i:CSV -headerRow:OFF "SELECT Field1, Field3 FROM Actors.txt WHERE Field3 LIKE 'M%'"
```

OUTPUT



OBSERVATION

The command above returns the first and third fields in the file whose records’ Field3 value starts from the letter ‘M’.