

# Lab Assignment



Cybersecurity Professional Program  
Digital Forensics Incident  
Response

## Log Analysis

**DFIR-09-L2**

**Event Viewer Tools**

## Lab Objective

Understand how to apply basic forensics actions on Event Viewer logs.

## Lab Mission

Examine the investigation process of Event Viewer by using SQL queries.

## Lab Duration

20–30 minutes

## Requirements

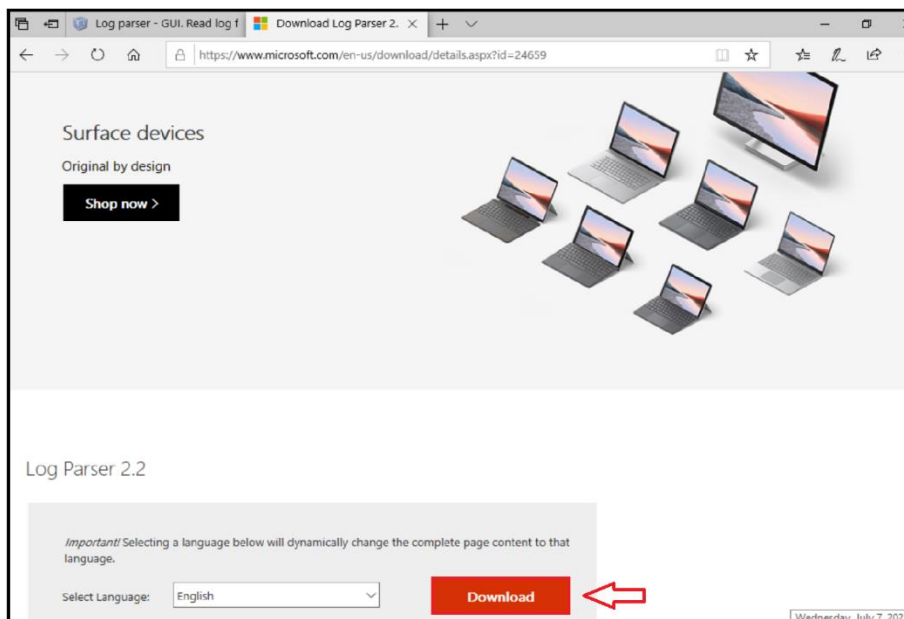
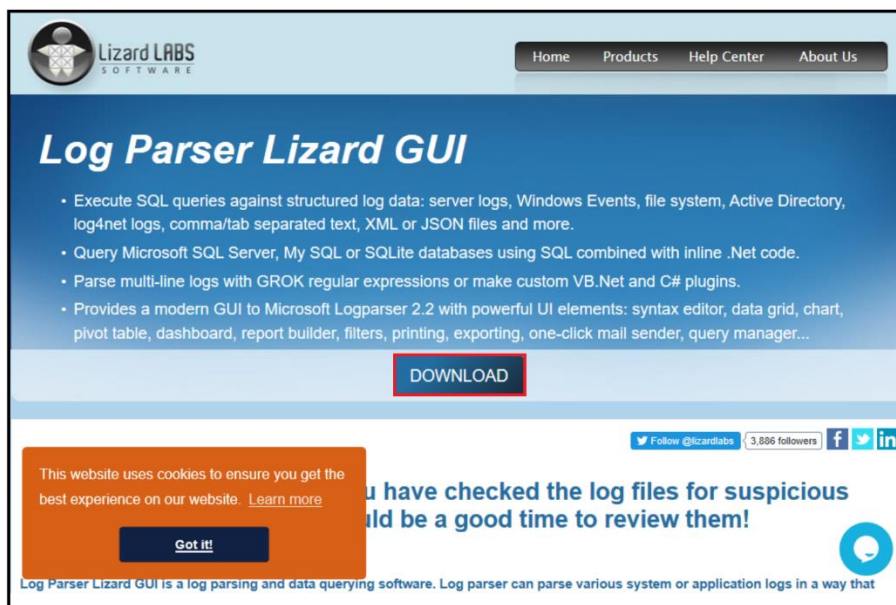
- Event logs from Windows Event Viewer
- Knowledge of basic SQL queries

## Resources

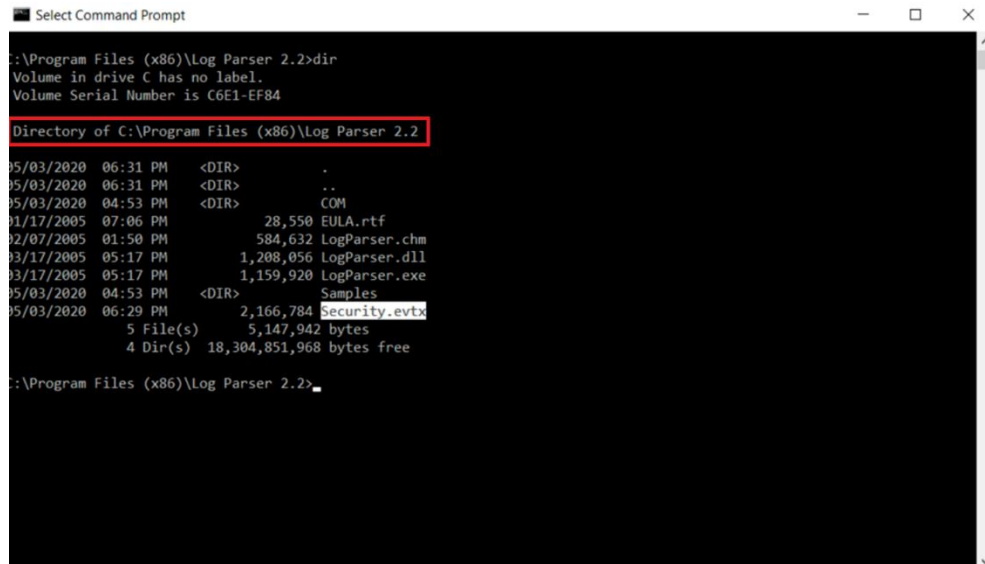
- Environment & Tools
  - Windows VM
- Extra Lab Files
  - ***Security.evtx***
- Extra Links
  - **Log Parser Lizard:**  
[http://www.lizard-labs.com/log\\_parser\\_lizard.aspx](http://www.lizard-labs.com/log_parser_lizard.aspx)
  - **Microsoft Log Parser 2.2:**  
<https://www.microsoft.com/en-us/download/details.aspx?id=24659>

## Lab Task 1: Microsoft Log Parser 2.2

- 1 Download **Microsoft Log Parser 2.2** and **Log Parser Lizard** to your Windows VM and install them.



- 2 Transfer the ***Security.evtx*** file to the following directory:  
***C:\Program Files (x86)\Log Parser 2.2\***  
Using the Administrative Command line, go to the path above.



```
Select Command Prompt
C:\Program Files (x86)\Log Parser 2.2>dir
Volume in drive C has no label.
Volume Serial Number is C6E1-EF84

Directory of C:\Program Files (x86)\Log Parser 2.2

05/03/2020  06:31 PM  <DIR>          .
05/03/2020  06:31 PM  <DIR>          ..
05/03/2020  04:53 PM  <DIR>          COM
01/17/2005  07:06 PM                28,550 EULA.rtf
02/07/2005  01:50 PM            584,632 LogParser.chm
03/17/2005  05:17 PM          1,208,056 LogParser.dll
03/17/2005  05:17 PM          1,159,920 LogParser.exe
05/03/2020  04:53 PM  <DIR>          Samples
05/03/2020  06:29 PM          2,166,784 Security.evtx
               5 File(s)          5,147,942 bytes
               4 Dir(s) 18,304,851,968 bytes free

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

- Use **Log Parser 2.2** to query the Event Viewer file for all logs and export them to a CSV file. Use **Excel** to view the EventID column.

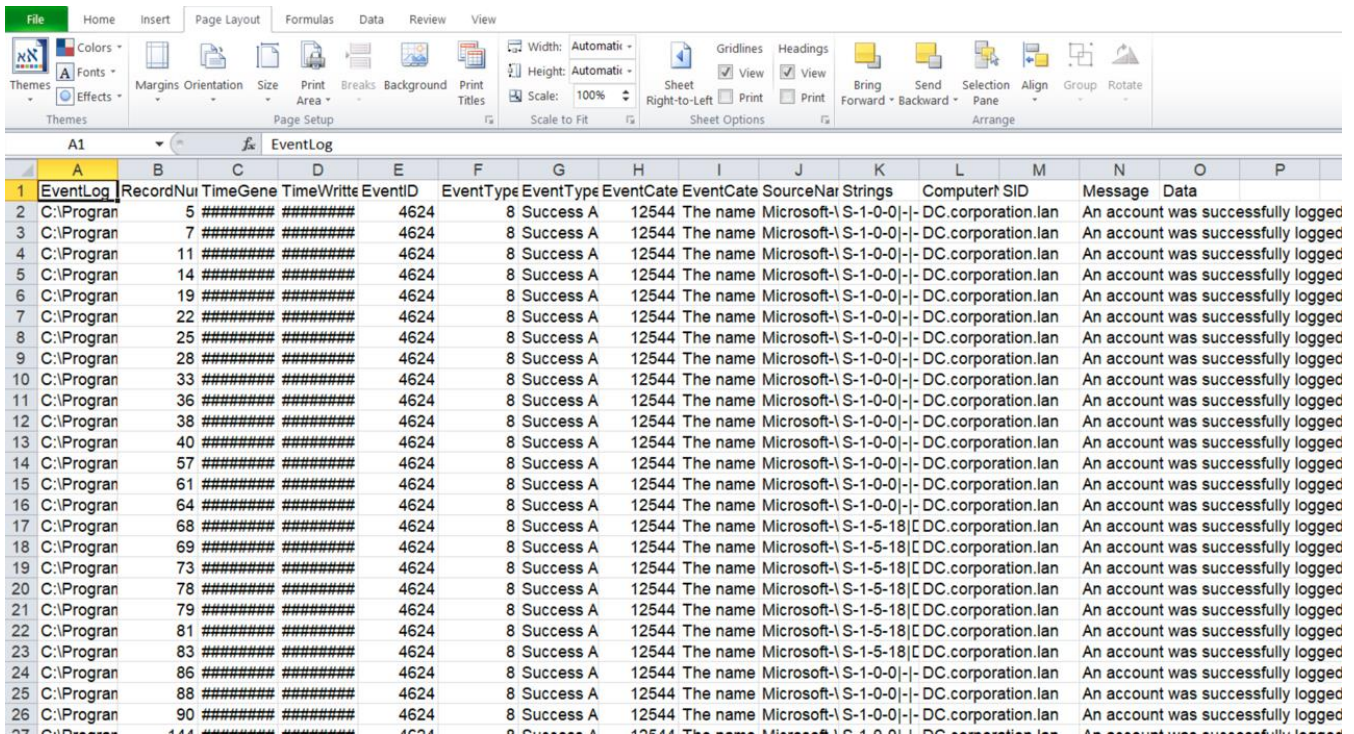
Use the following query:

**LogParser.exe -i:EVT -o:csv "SELECT \* FROM Security.evtx" > allLogs.csv**

EventLog	RecordNu	TimeGene	TimeWrit	EventID	EventType	EventTyp	EventCate	EventCate	SourceNai	Strings	Computer	SID	Message	Data
C:\Users\k	1	#####	#####	1102	8	Success A	104	The name Microsoft	S-1-5-21-2	DC.corporation.lan			The audit log was cleared. Subject: S	
C:\Users\k	2	#####	#####	4634	8	Success A	12545	The name Microsoft	S-1-5-18	[DC.corporation.lan			The description for Event ID 4634 in S	
C:\Users\k	3	#####	#####	4634	8	Success A	12545	The name Microsoft	S-1-5-18	[DC.corporation.lan			The description for Event ID 4634 in S	
C:\Users\k	4	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	
C:\Users\k	5	#####	#####	4624	8	Success A	12544	The name Microsoft	S-1-0-0	[DC.corporation.lan			The description for Event ID 4624 in S	
C:\Users\k	6	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	
C:\Users\k	7	#####	#####	4624	8	Success A	12544	The name Microsoft	S-1-0-0	[DC.corporation.lan			The description for Event ID 4624 in S	
C:\Users\k	8	#####	#####	4662	8	Success A	14080	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4662 in S	
C:\Users\k	9	#####	#####	4742	8	Success A	13825	The name Microsoft	-	DC.corporation.lan			The description for Event ID 4742 in S	
C:\Users\k	10	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	
C:\Users\k	11	#####	#####	4624	8	Success A	12544	The name Microsoft	S-1-0-0	[DC.corporation.lan			The description for Event ID 4624 in S	
C:\Users\k	12	#####	#####	4662	8	Success A	14080	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4662 in S	
C:\Users\k	13	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	
C:\Users\k	14	#####	#####	4624	8	Success A	12544	The name Microsoft	S-1-0-0	[DC.corporation.lan			The description for Event ID 4624 in S	
C:\Users\k	15	#####	#####	4634	8	Success A	12545	The name Microsoft	S-1-5-18	[DC.corporation.lan			The description for Event ID 4634 in S	
C:\Users\k	16	#####	#####	4662	8	Success A	14080	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4662 in S	
C:\Users\k	17	#####	#####	4634	8	Success A	12545	The name Microsoft	S-1-5-18	[DC.corporation.lan			The description for Event ID 4634 in S	
C:\Users\k	18	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	
C:\Users\k	19	#####	#####	4624	8	Success A	12544	The name Microsoft	S-1-0-0	[DC.corporation.lan			The description for Event ID 4624 in S	
C:\Users\k	20	#####	#####	4634	8	Success A	12545	The name Microsoft	S-1-5-18	[DC.corporation.lan			The description for Event ID 4634 in S	
C:\Users\k	21	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	
C:\Users\k	22	#####	#####	4624	8	Success A	12544	The name Microsoft	S-1-0-0	[DC.corporation.lan			The description for Event ID 4624 in S	
C:\Users\k	23	#####	#####	4634	8	Success A	12545	The name Microsoft	S-1-5-18	[DC.corporation.lan			The description for Event ID 4634 in S	
C:\Users\k	24	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	
C:\Users\k	25	#####	#####	4624	8	Success A	12544	The name Microsoft	S-1-0-0	[DC.corporation.lan			The description for Event ID 4624 in S	
C:\Users\k	26	#####	#####	4634	8	Success A	12545	The name Microsoft	S-1-5-18	[DC.corporation.lan			The description for Event ID 4634 in S	
C:\Users\k	27	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	
C:\Users\k	28	#####	#####	4624	8	Success A	12544	The name Microsoft	S-1-0-0	[DC.corporation.lan			The description for Event ID 4624 in S	
C:\Users\k	29	#####	#####	4634	8	Success A	12545	The name Microsoft	S-1-5-18	[DC.corporation.lan			The description for Event ID 4634 in S	
C:\Users\k	30	#####	#####	4662	8	Success A	14080	The name Microsoft	S-1-5-21-	DC.corporation.lan			The description for Event ID 4662 in S	
C:\Users\k	31	#####	#####	4739	8	Success A	13569	The name Microsoft	-	[CORPOFDC.corporation.lan			The description for Event ID 4739 in S	
C:\Users\k	32	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	
C:\Users\k	33	#####	#####	4624	8	Success A	12544	The name Microsoft	S-1-0-0	[DC.corporation.lan			The description for Event ID 4624 in S	
C:\Users\k	34	#####	#####	4634	8	Success A	12545	The name Microsoft	S-1-5-18	[DC.corporation.lan			The description for Event ID 4634 in S	
C:\Users\k	35	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	
C:\Users\k	36	#####	#####	4624	8	Success A	12544	The name Microsoft	S-1-0-0	[DC.corporation.lan			The description for Event ID 4624 in S	
C:\Users\k	37	#####	#####	4672	8	Success A	12548	The name Microsoft	S-1-5-	DC.corporation.lan			The description for Event ID 4672 in S	



- 4 Run **Log Parser 2.2** again to search for all logs that contain EventID 4624 and export the results to **Excel**. Use the following command: **LogParser.exe -i:EVT -o:csv "SELECT \* FROM 'security.evtx' WHERE EventID = '4624'" >successfulLogin.csv**

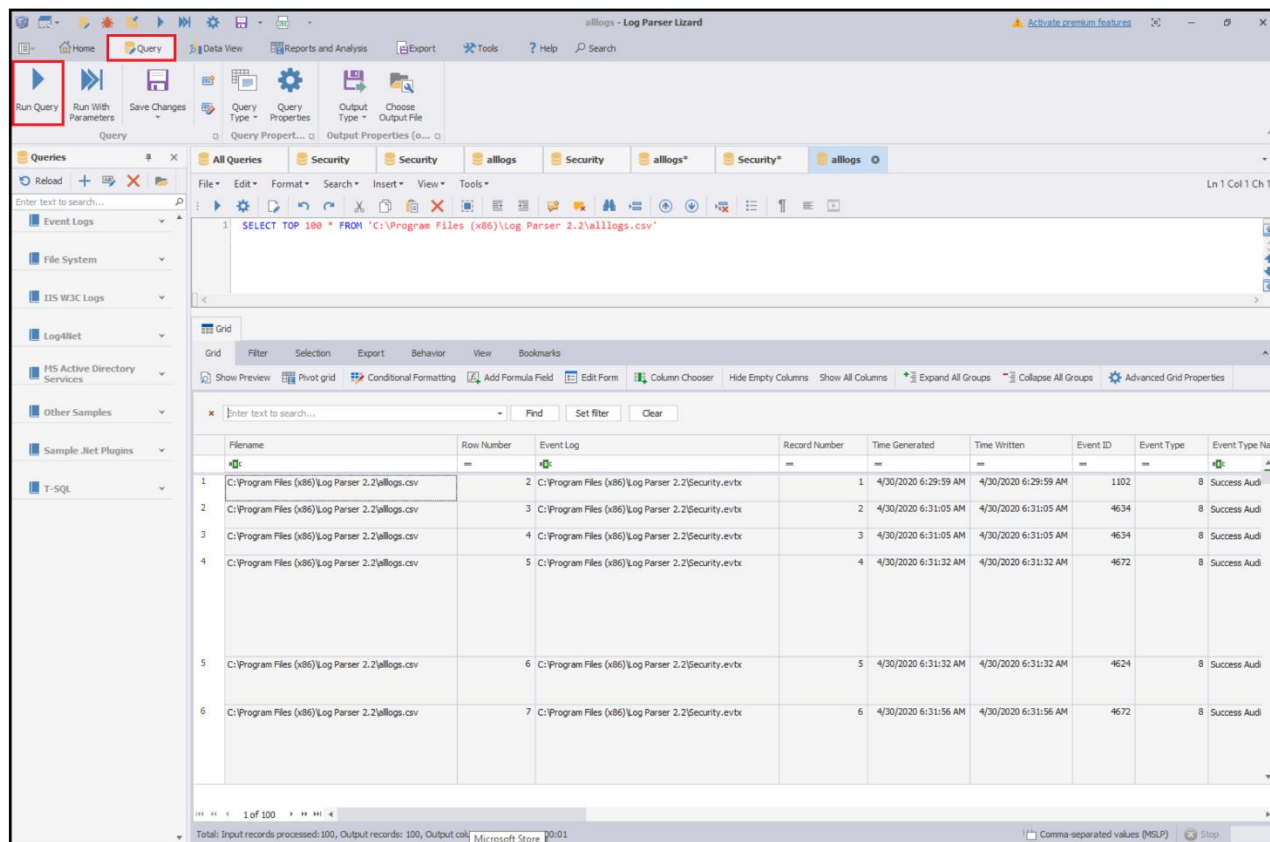


EventLog	RecordNumber	TimeGenerated	TimeWritten	EventID	EventType	EventCategory	EventSource	SourceName	Strings	ComputerName	Message
C:\Program	5	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	7	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	11	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	14	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	19	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	22	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	25	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	28	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	33	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	36	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	38	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	40	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	57	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	61	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	64	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	68	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-5-18 DC.corporation.lan		An account was successfully logged
C:\Program	69	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-5-18 DC.corporation.lan		An account was successfully logged
C:\Program	73	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-5-18 DC.corporation.lan		An account was successfully logged
C:\Program	78	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-5-18 DC.corporation.lan		An account was successfully logged
C:\Program	79	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-5-18 DC.corporation.lan		An account was successfully logged
C:\Program	81	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-5-18 DC.corporation.lan		An account was successfully logged
C:\Program	83	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-5-18 DC.corporation.lan		An account was successfully logged
C:\Program	86	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	88	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	90	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged
C:\Program	94	#####	#####	4624	8	Success A	12544	The name Microsoft\	S-1-0-0 -  DC.corporation.lan		An account was successfully logged

- 5 Now use **Log Parser 2.2** to search for a logon event with logon type 3. Use the following command: **LogParser.exe -i:EVT -o:csv "SELECT \* FROM 'Security.evtx' WHERE EventID = '4624' and Message like '%Logon Type: 3%'" > logonType3.csv**

## Lab Task 2: Log Parser Lizard

- 1 Open the **Log Parser Lizard** tool and then the **allLogs.csv** file for investigation. Run the built-in query. To open the program, click **Start** and search for **LPL Quick Query**. Use the query **SELECT TOP 100 \* FROM 'C:\Program Files (x86)\Log Parser 2.2\allLogs.csv'**



- 2 Query the file to output all failed login attempts by using **SELECT \* FROM 'C:\Program Files (x86)\Log Parser 2.2\allLogs.csv' WHERE EventID = '4625'**
- 3 Query the file to output created users in the logs with **SELECT TOP 100 \* FROM 'C:\Program Files (x86)\Log Parser 2.2\allLogs.csv' WHERE EventID = '4720'**  
How many users were created? How many users were created by the admin, and how many users were created by a user? Which user(s) were being used to create other accounts?

- 
- 4 Which user(s) were deactivated? Use the query to find ***SELECT TOP 100 \* FROM 'C:\Program Files (x86)\Log Parser 2.2\allLogs.csv' WHERE EventID = '4720'***
  - 5 Use the file parsed from the command line, ***SELECT TOP 100 \* FROM 'C:\Program Files (x86)\Log Parser 2.2\SuccessfulLogin.csv'***
  - 6 Use the file parsed from the command line, ***SELECT TOP 100 \* FROM 'C:\Program Files (x86)\Log Parser 2.2\LogonType3.csv'***
  - 7 Try to determine if a Brute-force event occurred and note your findings.