Windows Triaging with Powershell - Part 1 - Parsing Event Logs

This is the part 1 for Triaging a Windows system with Powershell. On a Windows machine, Event Logs play an important role in determining a timeline of various User and System activities by integrating logging information and assessing different EntryTypes comprising the logs to reveal the behavior of each activity on the machine.

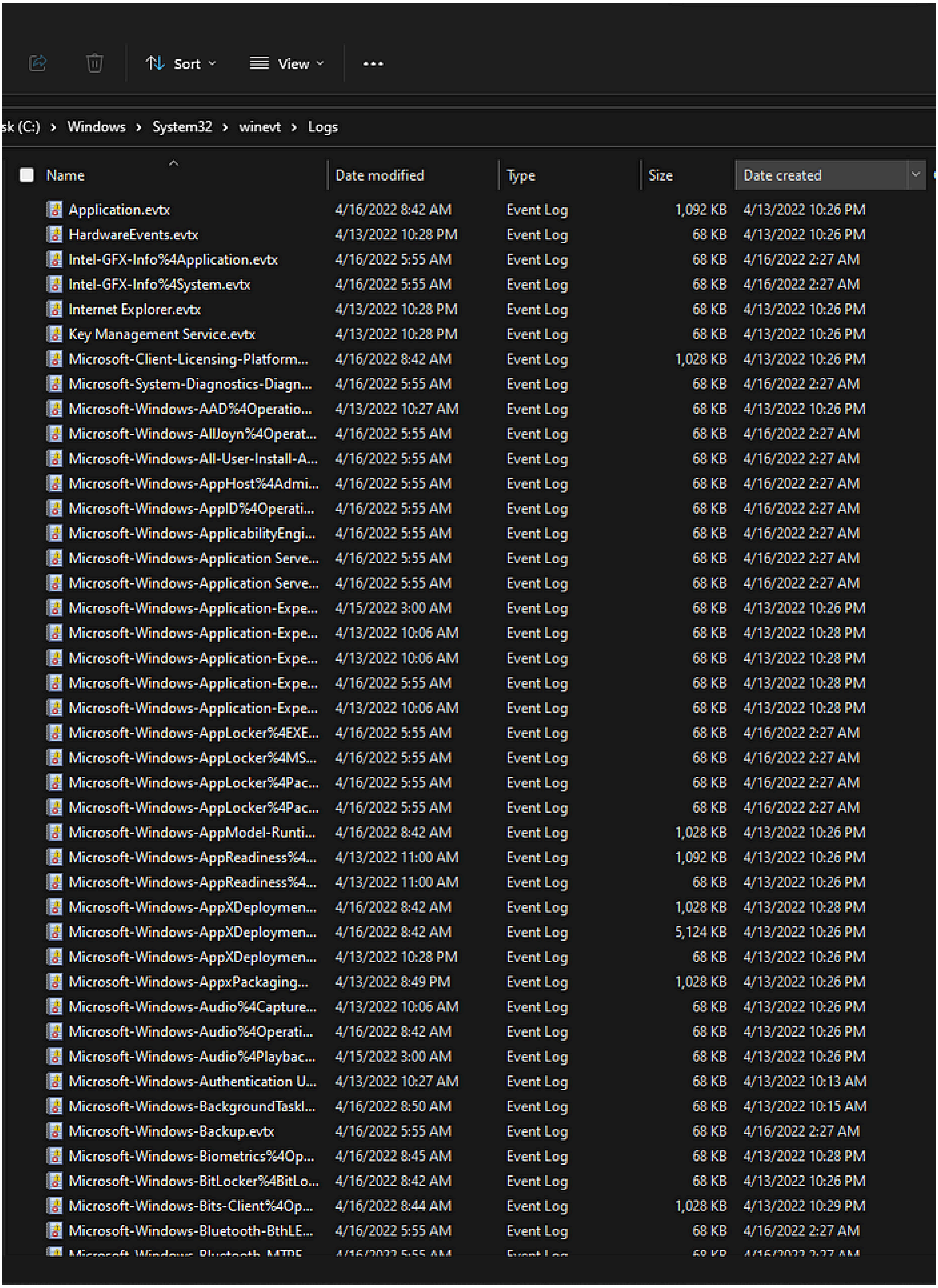
There are many features available in Windows Powershell to analyze Event Logs, parse the data and create report. In this blog, we will look at some of the Powershell functions to perform these activities.

We will now look at how to parse Windows Event Logs with Powershell commands and create a HTML Report.

1. What is Event Logging?

As per Microsoft documentation, "Many applications record errors and events in proprietary error logs, each with their own format and user interface. Event logging provides a standard standard, centralized way for applications to record important software and hardware events. The event logging service records events from various sources and stored them in single collection called an ***Event Log.***"

> Default location for Windows Event Logs
>
> C:\Windows\System32\winevt\Logs



sk (C:) › Windows › System32 › winevt › Logs

Name	Date modified	Type	Size	Date created
Application.evtx	4/16/2022 8:42 AM	Event Log	1,092 KB	4/13/2022 10:26 PM
HardwareEvents.evtx	4/13/2022 10:28 PM	Event Log	68 KB	4/13/2022 10:26 PM
Intel-GFX-Info%4Application.evtx	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Intel-GFX-Info%4System.evtx	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Internet Explorer.evtx	4/13/2022 10:28 PM	Event Log	68 KB	4/13/2022 10:26 PM
Key Management Service.evtx	4/13/2022 10:28 PM	Event Log	68 KB	4/13/2022 10:26 PM
Microsoft-Client-Licensing-Platform...	4/16/2022 8:42 AM	Event Log	1,028 KB	4/13/2022 10:26 PM
Microsoft-System-Diagnostics-Diagn...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-AAD%4Operatio...	4/13/2022 10:27 AM	Event Log	68 KB	4/13/2022 10:26 PM
Microsoft-Windows-AllJoyn%4Operat...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-All-User-Install-A...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-AppHost%4Admi...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-AppID%4Operati...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-ApplicabilityEngi...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-Application Serve...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-Application Serve...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-Application-Expe...	4/15/2022 3:00 AM	Event Log	68 KB	4/13/2022 10:26 PM
Microsoft-Windows-Application-Expe...	4/13/2022 10:06 AM	Event Log	68 KB	4/13/2022 10:28 PM
Microsoft-Windows-Application-Expe...	4/13/2022 10:06 AM	Event Log	68 KB	4/13/2022 10:28 PM
Microsoft-Windows-Application-Expe...	4/16/2022 5:55 AM	Event Log	68 KB	4/13/2022 10:28 PM
Microsoft-Windows-Application-Expe...	4/13/2022 10:06 AM	Event Log	68 KB	4/13/2022 10:28 PM
Microsoft-Windows-AppLocker%4EXE...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-AppLocker%4MS...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-AppLocker%4Pac...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-AppLocker%4Pac...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-AppModel-Runti...	4/16/2022 8:42 AM	Event Log	1,028 KB	4/13/2022 10:26 PM
Microsoft-Windows-AppReadiness%4...	4/13/2022 11:00 AM	Event Log	1,092 KB	4/13/2022 10:26 PM
Microsoft-Windows-AppReadiness%4...	4/13/2022 11:00 AM	Event Log	68 KB	4/13/2022 10:26 PM
Microsoft-Windows-AppXDeploymen...	4/16/2022 8:42 AM	Event Log	1,028 KB	4/13/2022 10:28 PM
Microsoft-Windows-AppXDeploymen...	4/16/2022 8:42 AM	Event Log	5,124 KB	4/13/2022 10:26 PM
Microsoft-Windows-AppXDeploymen...	4/13/2022 10:28 PM	Event Log	68 KB	4/13/2022 10:26 PM
Microsoft-Windows-AppxPackaging...	4/13/2022 8:49 PM	Event Log	1,028 KB	4/13/2022 10:26 PM
Microsoft-Windows-Audio%4Capture...	4/13/2022 10:06 AM	Event Log	68 KB	4/13/2022 10:26 PM
Microsoft-Windows-Audio%4Operati...	4/16/2022 8:42 AM	Event Log	68 KB	4/13/2022 10:26 PM
Microsoft-Windows-Audio%4Playbac...	4/15/2022 3:00 AM	Event Log	68 KB	4/13/2022 10:26 PM
Microsoft-Windows-Authentication U...	4/13/2022 10:27 AM	Event Log	68 KB	4/13/2022 10:13 AM
Microsoft-Windows-BackgroundTaskI...	4/16/2022 8:50 AM	Event Log	68 KB	4/13/2022 10:15 AM
Microsoft-Windows-Backup.evtx	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-Biometrics%4Op...	4/16/2022 8:45 AM	Event Log	68 KB	4/13/2022 10:28 PM
Microsoft-Windows-BitLocker%4BitLo...	4/16/2022 8:42 AM	Event Log	68 KB	4/13/2022 10:26 PM
Microsoft-Windows-Bits-Client%4Op...	4/16/2022 8:44 AM	Event Log	1,028 KB	4/13/2022 10:29 PM
Microsoft-Windows-Bluetooth-BthLE...	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM
Microsoft-Windows-Bluetooth-MTPE	4/16/2022 5:55 AM	Event Log	68 KB	4/16/2022 2:27 AM

Out of these number of Event logs, major Windows Event logs are

1.1. Application Logs

- These logs are generated by applications or programs

1.2. System Logs

- These logs are generated by Windows system components

1.3. Security Logs

- These logs are generated by Windows security events like login attempts or deleting objects etc.

2. What are different Event Types?

There are 5 types of events that are logged:

2.1. Error

- Event indicates a significant problem such as loss of data or loss of functionality

2.2. Warning

- Indicate a possible future problem. If an application can recover from event without loss of functionality or data, it can generally classify event as Warning event

2.3. Information

- Describes successful operation of application, driver or service

2.4. Success Audit

- Records an audited security access attempt that is successful

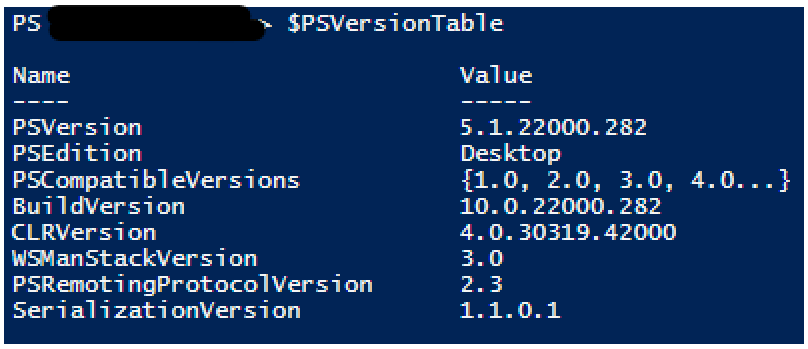
2.5. Failure Audit

- Records an audited security access attempt that fails

3. How Powershell is used for parsing Log Files?

These functions are tested on Powershell version 5.1 You may check your Powershell version using command

```
$PSVersionTable
```



```
PS [redacted]> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      5.1.22000.282
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.22000.282
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1
```

> Before executing Powershell scripts, it's necessary to Bypass or Unrestrict the ExecutionPolicy on Powershell by the following command

```
Set-ExecutionPolicy Unrestricted or Set-ExecutionPolicy Bypass
```

3.1. Live System Logs Parsing

On a Live Windows system, open a Powershell Windows. If possible,then open with administrative privileges. You can open the Powershell Window with admin privileges by 2 methods:

First Method

- Press Win+R, this will open Run dialog on your screen
- Type 'powershell', and press Ctrl+Shift+Enter
- This will open the Powershell window with Admin Privileges

Second Method

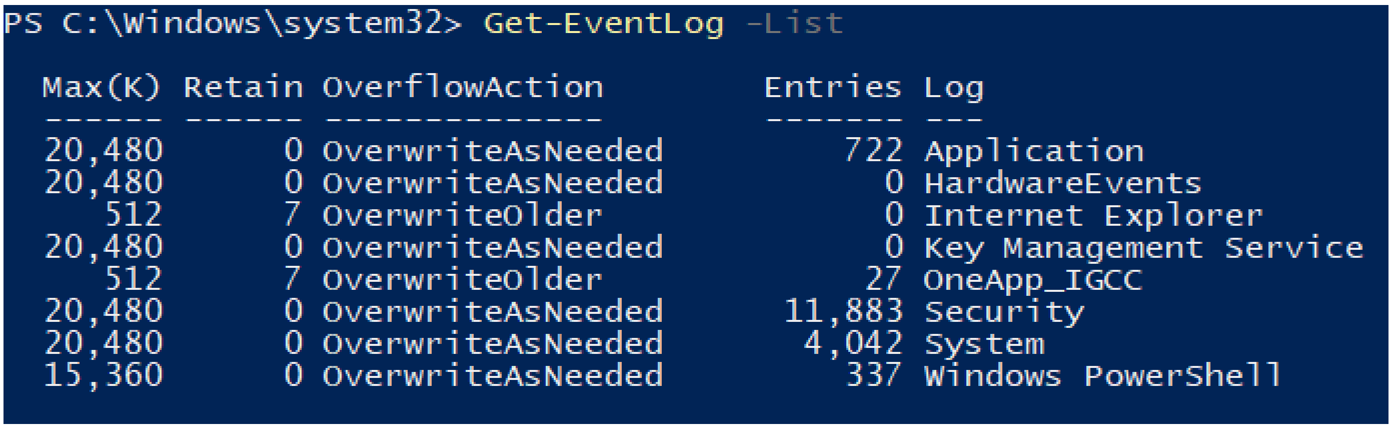
- Press Win+R, open the Run dialog on the screen
- Type 'powershell' and hit Enter
- On the powershell window, type the following command on the powershell terminal "*Start-Process powershell -Verb Runas*"
- This will open Powershell window again with Admin Privileges

Now, our Powershell Window is up and running with Administrative Privileges, we are good to go with parsing the Event Logs.

First task would be checking the entries in our major Event Log files. For this, on the Powershell window, type the following command

```
Get-EventLog -List
```

The output of this command will display information about the major Event Logs with some of the information as displayed in the below screenshot


```
PS C:\Windows\system32> Get-EventLog -List

  Max(K) Retain OverflowAction        Entries Log
  ------ ------ --------------        ------- ---
  20,480      0 OverwriteAsNeeded         722 Application
  20,480      0 OverwriteAsNeeded           0 HardwareEvents
     512      7 OverwriteOlder              0 Internet Explorer
  20,480      0 OverwriteAsNeeded           0 Key Management Service
     512      7 OverwriteOlder             27 OneApp_IGCC
  20,480      0 OverwriteAsNeeded      11,883 Security
  20,480      0 OverwriteAsNeeded       4,042 System
  15,360      0 OverwriteAsNeeded         337 Windows PowerShell
```

As mentioned in the screenshot, our major Event Logs are Application, HardwareEvents, InternetExplorer, KeyManagementServices, OneApp_IGCC, Security, System, WindowsPowershell.

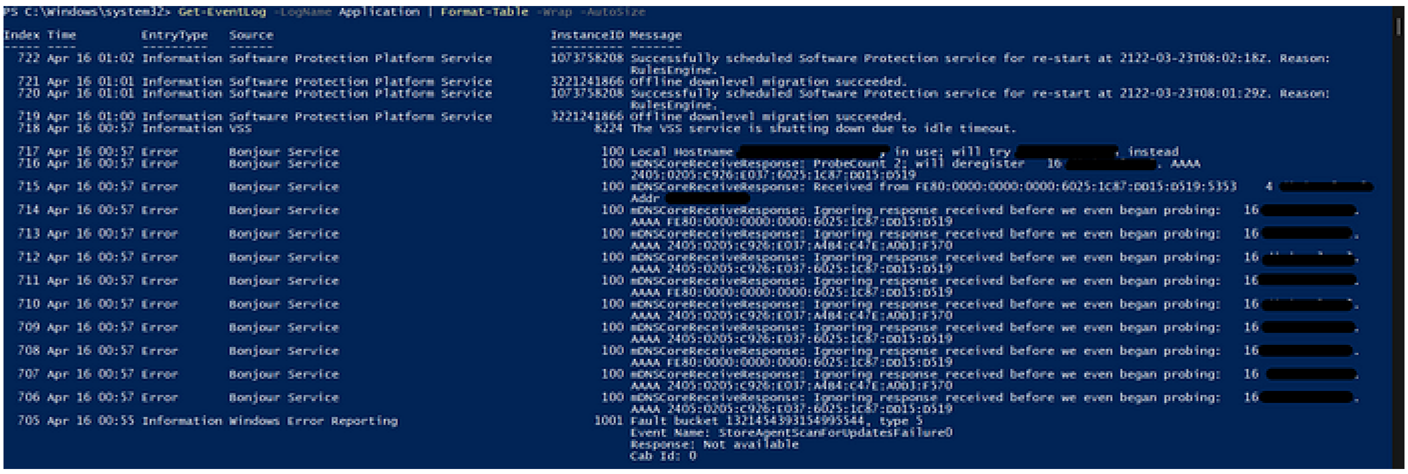
For the following Logs, we have Entries field which shows the number of entries that are written in the particular Log. As there are no entries defined in HardwareEvents, InternetExplorer and KeyManagementService, our target would be finding the Log entries for the rest of the Log files.

3.2. Application Logs Parsing

To examine the Application Logs from Powershell, enter the following command in the Powershell window:

```
Get-EventLog -LogName Application | Format-Table -Wrap -AutoSize
```

This will display all the entries within the Application Logs on Powershell Window in Tabular format. Flags 'Wrap' & 'AutoSize' will allow to display the full content on the Powershell Windows itself.

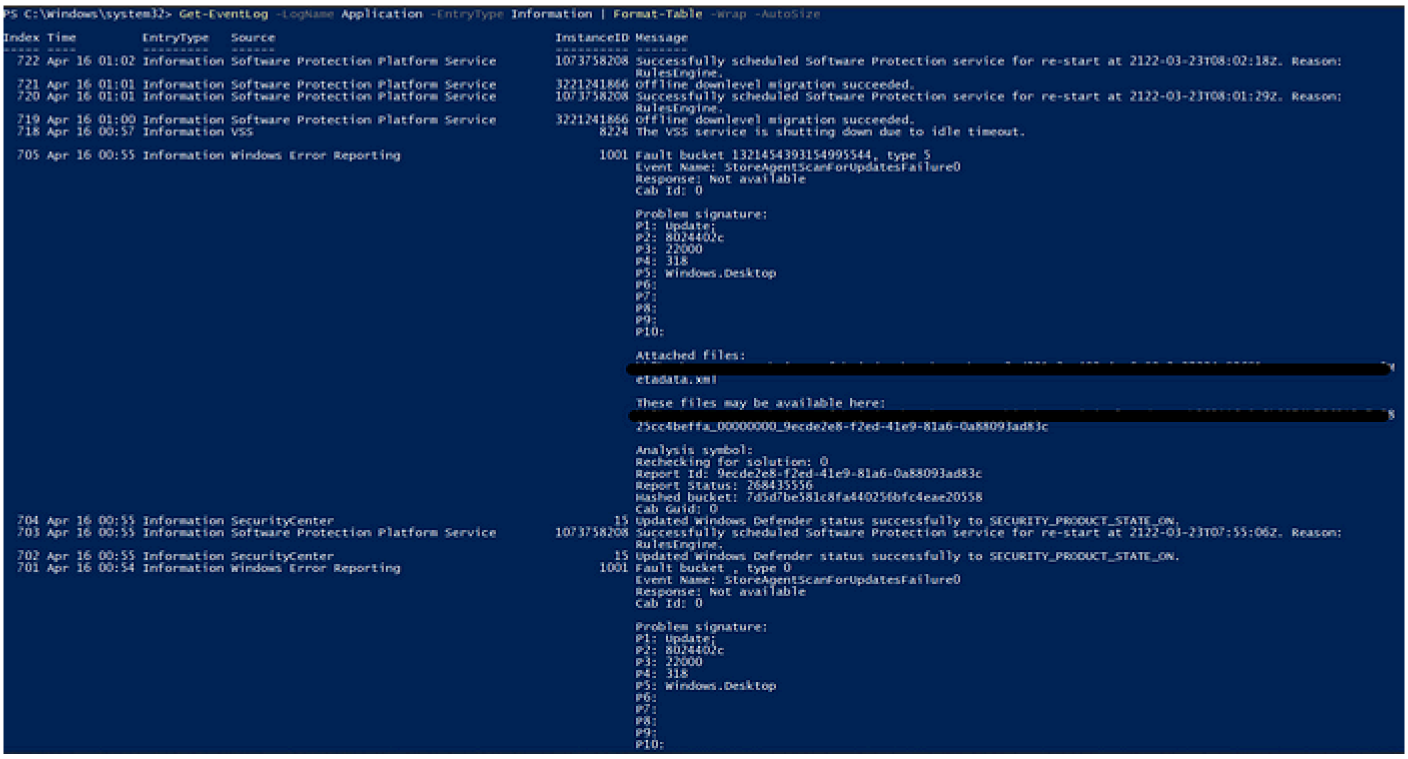


```
PS C:\Windows\system32> Get-EventLog -LogName Application | Format-Table -Wrap -AutoSize

Index Time         EntryType   Source                                    InstanceID Message
----- ----         ---------   ------                                    ---------- -------
  722 Apr 16 01:02 Information Software Protection Platform Service      1073758208 Successfully scheduled Software Protection service for re-start at 2122-03-23T08:02:18Z. Reason:
                                                                                    RulesEngine.
  721 Apr 16 01:01 Information Software Protection Platform Service      3221241866 Offline downlevel migration succeeded.
  720 Apr 16 01:01 Information Software Protection Platform Service      1073758208 Successfully scheduled Software Protection service for re-start at 2122-03-23T08:01:29Z. Reason:
                                                                                    RulesEngine.
  719 Apr 16 01:00 Information Software Protection Platform Service      3221241866 Offline downlevel migration succeeded.
  718 Apr 16 00:57 Information VSS                                             8224 The VSS service is shutting down due to idle timeout.

  717 Apr 16 00:57 Error       Bonjour Service                                  100 Local Hostname [redacted], in use; will try [redacted], instead
  716 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: ProbeCount 2; will deregister   16 [redacted]. AAAA
                                                                                    2405:0205:C926:E037:6025:1C87:DD15:D519
  715 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: Received from FE80:0000:0000:0000:6025:1C87:DD15:D519:5353   4 [redacted]
                                                                                    Addr [redacted]
  714 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: Ignoring response received before we even began probing:   16 [redacted].
                                                                                    AAAA FE80:0000:0000:0000:6025:1C87:DD15:D519
  713 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: Ignoring response received before we even began probing:   16 [redacted].
                                                                                    AAAA 2405:0205:C926:E037:A4B4:C47E:A0D3:F570
  712 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: Ignoring response received before we even began probing:   16 [redacted].
                                                                                    AAAA 2405:0205:C926:E037:6025:1C87:DD15:D519
  711 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: Ignoring response received before we even began probing:   16 [redacted].
                                                                                    AAAA FE80:0000:0000:0000:6025:1C87:DD15:D519
  710 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: Ignoring response received before we even began probing:   16 [redacted].
                                                                                    AAAA 2405:0205:C926:E037:A4B4:C47E:A0D3:F570
  709 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: Ignoring response received before we even began probing:   16 [redacted].
                                                                                    AAAA 2405:0205:C926:E037:6025:1C87:DD15:D519
  708 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: Ignoring response received before we even began probing:   16 [redacted].
                                                                                    AAAA FE80:0000:0000:0000:6025:1C87:DD15:D519
  707 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: Ignoring response received before we even began probing:   16 [redacted].
                                                                                    AAAA 2405:0205:C926:E037:A4B4:C47E:A0D3:F570
  706 Apr 16 00:57 Error       Bonjour Service                                  100 mDNSCoreReceiveResponse: Ignoring response received before we even began probing:   16 [redacted].
                                                                                    AAAA 2405:0205:C926:E037:6025:1C87:DD15:D519
  705 Apr 16 00:55 Information Windows Error Reporting                         1001 Fault bucket 1321454393154995544, type 5
                                                                                    Event Name: StoreAgentScanForUpdatesFailure0
                                                                                    Response: Not available
                                                                                    Cab Id: 0
```

Next, we can display the entries with specific EntryType. For example, if we want to display only the Application Logs with "Information" EntryType, type the following command in Powershell window

```
Get-EventLog -LogName Application -EntryType Information | Format-Table -Wrap -AutoSize
```

This command will display only the Information EntryType within the Application Logs. The below screenshot displays the output of the above command.

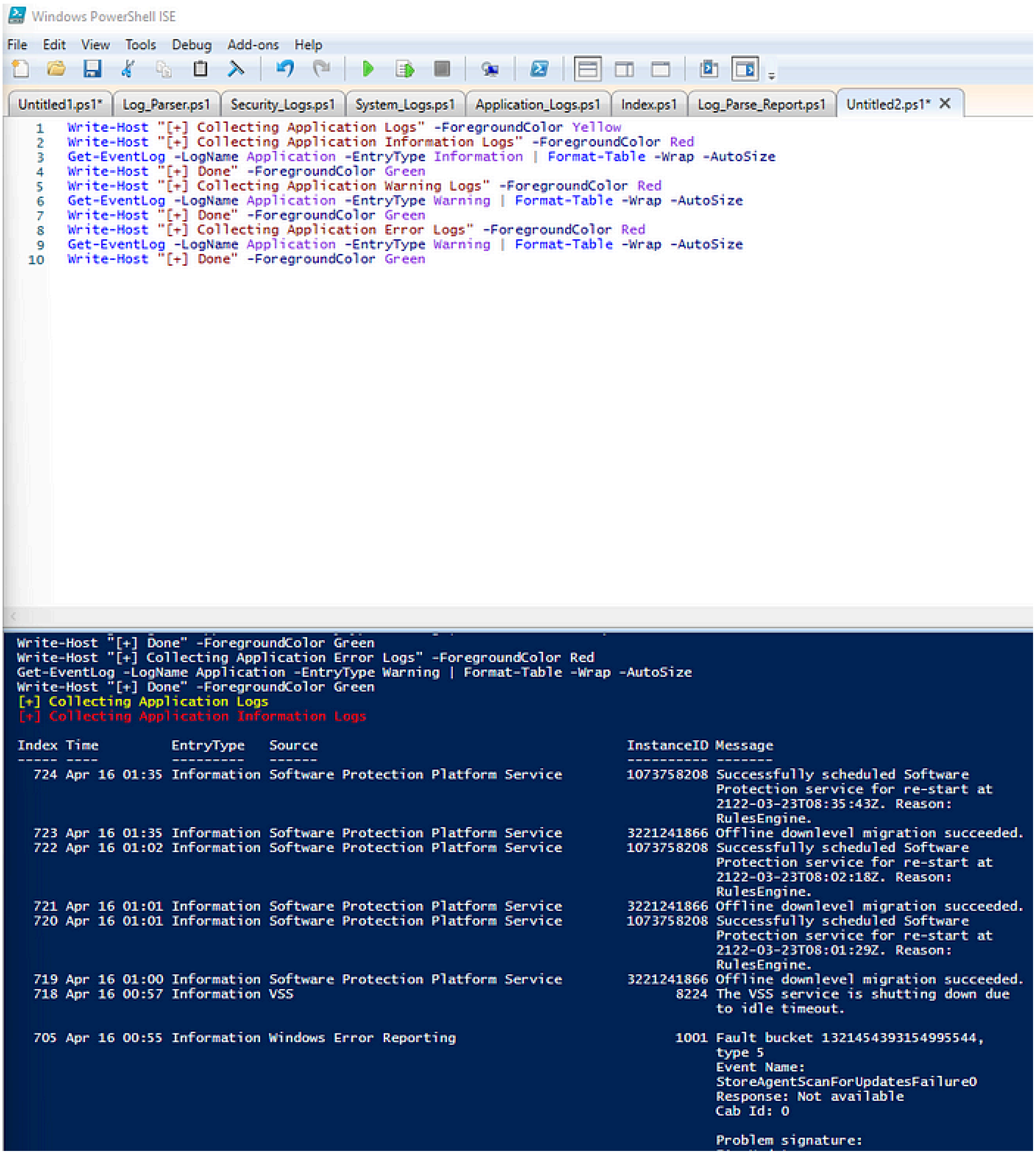


```
PS C:\Windows\system32> Get-EventLog -LogName Application -EntryType Information | Format-Table -Wrap -AutoSize

Index Time         EntryType   Source                                    InstanceID Message
----- ----         ---------   ------                                    ---------- -------
  722 Apr 16 01:02 Information Software Protection Platform Service      1073758208 Successfully scheduled Software Protection service for re-start at 2122-03-23T08:02:18Z. Reason:
                                                                                    RulesEngine.
  721 Apr 16 01:01 Information Software Protection Platform Service      3221241866 Offline downlevel migration succeeded.
  720 Apr 16 01:01 Information Software Protection Platform Service      1073758208 Successfully scheduled Software Protection service for re-start at 2122-03-23T08:01:29Z. Reason:
                                                                                    RulesEngine.
  719 Apr 16 01:00 Information Software Protection Platform Service      3221241866 Offline downlevel migration succeeded.
  718 Apr 16 00:57 Information VSS                                             8224 The VSS service is shutting down due to idle timeout.

  705 Apr 16 00:55 Information Windows Error Reporting                         1001 Fault bucket 1321454393154995544, type 5
                                                                                    Event Name: StoreAgentScanForUpdatesFailure0
                                                                                    Response: Not available
                                                                                    Cab Id: 0

                                                                                    Problem signature:
                                                                                    P1: Update;
                                                                                    P2: 8024402c
                                                                                    P3: 22000
                                                                                    P4: 318
                                                                                    P5: Windows.Desktop
                                                                                    P6:
                                                                                    P7:
                                                                                    P8:
                                                                                    P9:
                                                                                    P10:

                                                                                    Attached files:
                                                                                    [redacted]
                                                                                    etadata.xml

                                                                                    These files may be available here:
                                                                                    [redacted]
                                                                                    25cc4beffa_00000000_9ecde2e8-f2ed-41e9-81a6-0a88093ad83c

                                                                                    Analysis symbol:
                                                                                    Rechecking for solution: 0
                                                                                    Report Id: 9ecde2e8-f2ed-41e9-81a6-0a88093ad83c
                                                                                    Report Status: 268435556
                                                                                    Hashed bucket: 7d5d7be581c8fa440256bfc4eae20558
                                                                                    Cab Guid: 0
  704 Apr 16 00:55 Information SecurityCenter                                    15 Updated Windows Defender status successfully to SECURITY_PRODUCT_STATE_ON.
  703 Apr 16 00:55 Information Software Protection Platform Service      1073758208 Successfully scheduled Software Protection service for re-start at 2122-03-23T07:55:06Z. Reason:
                                                                                    RulesEngine.
  702 Apr 16 00:55 Information SecurityCenter                                    15 Updated Windows Defender status successfully to SECURITY_PRODUCT_STATE_ON.
  701 Apr 16 00:54 Information Windows Error Reporting                         1001 Fault bucket , type 0
                                                                                    Event Name: StoreAgentScanForUpdatesFailure0
                                                                                    Response: Not available
                                                                                    Cab Id: 0

                                                                                    Problem signature:
                                                                                    P1: Update;
                                                                                    P2: 8024402c
                                                                                    P3: 22000
                                                                                    P4: 318
                                                                                    P5: Windows.Desktop
                                                                                    P6:
                                                                                    P7:
                                                                                    P8:
                                                                                    P9:
                                                                                    P10:
```

Using the EventViewer, I discovered that there are only 3 EntryTypes in Application Logs i.e. "Information","Warning" & "Error". To automate this process, we can use a Powershell script to perform all these actions at once.

Save the script in desired directory after copying the commands in Powershell ISE

```
Write-Host "Collecting Application Logs" -ForegroundColor Yellow
Write-Host "Collecting Application Information Logs" -ForegroundColor Red

Get-EventLog -LogName Application -EntryType Information | Format-Table -Wrap -
AutoSize

Write-Host "Done" -ForegroundColor Green
Write-Host "Collecting Application Warning Logs" -ForegroundColor Red

Get-EventLog -LogName Application -EntryType Warning | Format-Table -Wrap -AutoSize

Write-Host "Done" -ForegroundColor Green
Write-Host "Collecting Application Error Logs" -ForegroundColor Red

Get-EventLog -LogName Application -EntryType Warning | Format-Table -Wrap -AutoSize

Write-Host "Done" -ForegroundColor Green
```



Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* Log_Parser.ps1 Security_Logs.ps1 System_Logs.ps1 Application_Logs.ps1 Index.ps1 Log_Parse_Report.ps1 Untitled2.ps1*

```
Write-Host "[+] Collecting Application Logs" -ForegroundColor Yellow
Write-Host "[+] Collecting Application Information Logs" -ForegroundColor Red
Get-EventLog -LogName Application -EntryType Information | Format-Table -Wrap -AutoSize
Write-Host "[+] Done" -ForegroundColor Green
Write-Host "[+] Collecting Application Warning Logs" -ForegroundColor Red
Get-EventLog -LogName Application -EntryType Warning | Format-Table -Wrap -AutoSize
Write-Host "[+] Done" -ForegroundColor Green
Write-Host "[+] Collecting Application Error Logs" -ForegroundColor Red
Get-EventLog -LogName Application -EntryType Warning | Format-Table -Wrap -AutoSize
Write-Host "[+] Done" -ForegroundColor Green
```

```
Write-Host "[+] Done" -ForegroundColor Green
Write-Host "[+] Collecting Application Error Logs" -ForegroundColor Red
Get-EventLog -LogName Application -EntryType Warning | Format-Table -Wrap -AutoSize
Write-Host "[+] Done" -ForegroundColor Green
[+] Collecting Application Logs
[+] Collecting Application Information Logs

Index Time         EntryType   Source                                 InstanceID Message
----- ----         ---------   ------                                 ---------- -------
  724 Apr 16 01:35 Information Software Protection Platform Service   1073758208 Successfully scheduled Software
                                                                                 Protection service for re-start at
                                                                                 2122-03-23T08:35:43Z. Reason:
                                                                                 RulesEngine.
  723 Apr 16 01:35 Information Software Protection Platform Service   3221241866 Offline downlevel migration succeeded.
  722 Apr 16 01:02 Information Software Protection Platform Service   1073758208 Successfully scheduled Software
                                                                                 Protection service for re-start at
                                                                                 2122-03-23T08:02:18Z. Reason:
                                                                                 RulesEngine.
  721 Apr 16 01:01 Information Software Protection Platform Service   3221241866 Offline downlevel migration succeeded.
  720 Apr 16 01:01 Information Software Protection Platform Service   1073758208 Successfully scheduled Software
                                                                                 Protection service for re-start at
                                                                                 2122-03-23T08:01:29Z. Reason:
                                                                                 RulesEngine.
  719 Apr 16 01:00 Information Software Protection Platform Service   3221241866 Offline downlevel migration succeeded.
  718 Apr 16 00:57 Information VSS                                          8224 The VSS service is shutting down due
                                                                                 to idle timeout.

  705 Apr 16 00:55 Information Windows Error Reporting                      1001 Fault bucket 1321454393154995544,
                                                                                 type 5
                                                                                 Event Name:
                                                                                 StoreAgentScanForUpdatesFailure0
                                                                                 Response: Not available
                                                                                 Cab Id: 0

                                                                                 Problem signature:
```

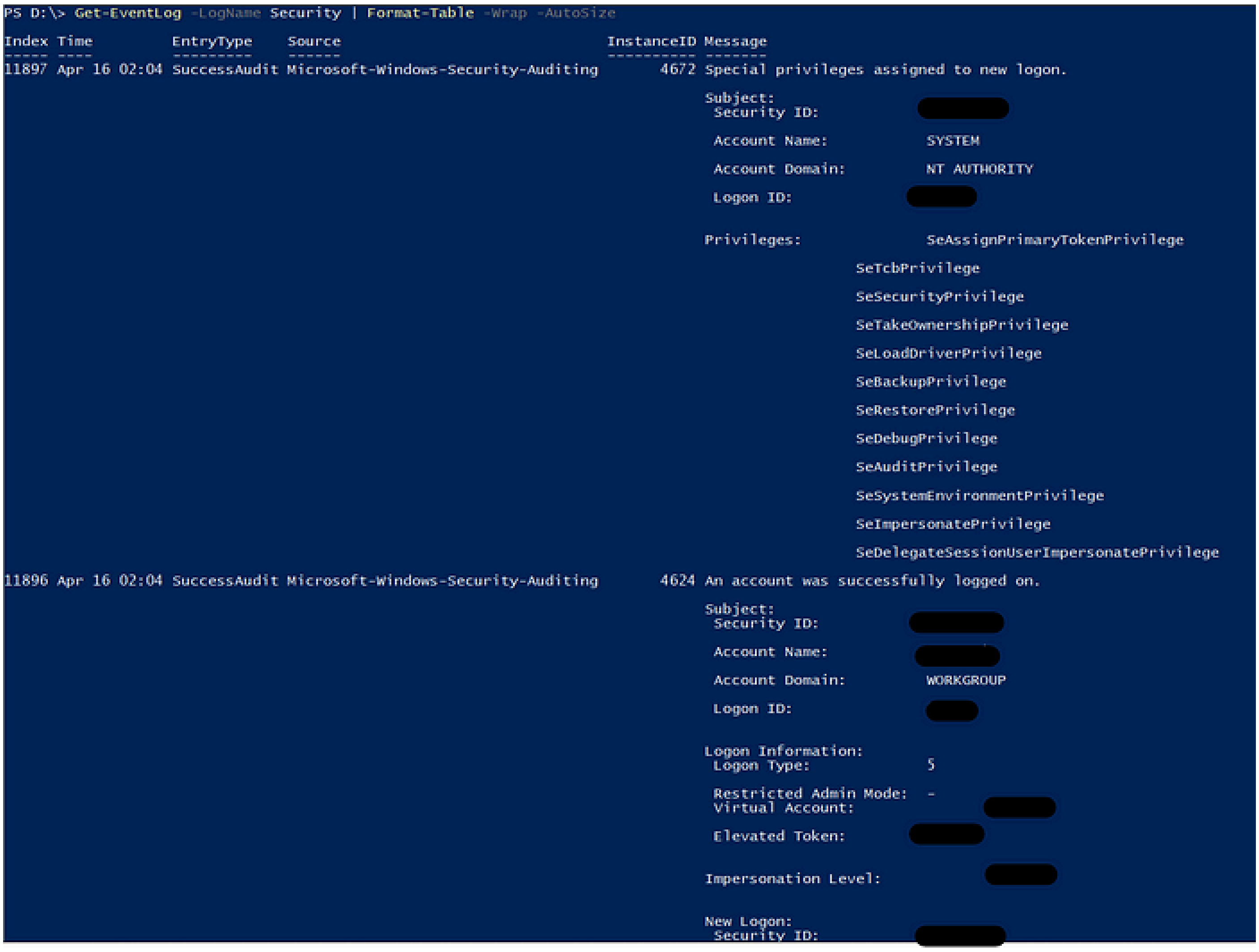
3.3. Security Logs Parsing

In order to parse Security logs, the command would remain the same as it was for parsing Application logs.

> **Note:** Parsing Security Logs would require Administrative Privileges otherwise you would see access denied error

Paste the following command in Powershell window

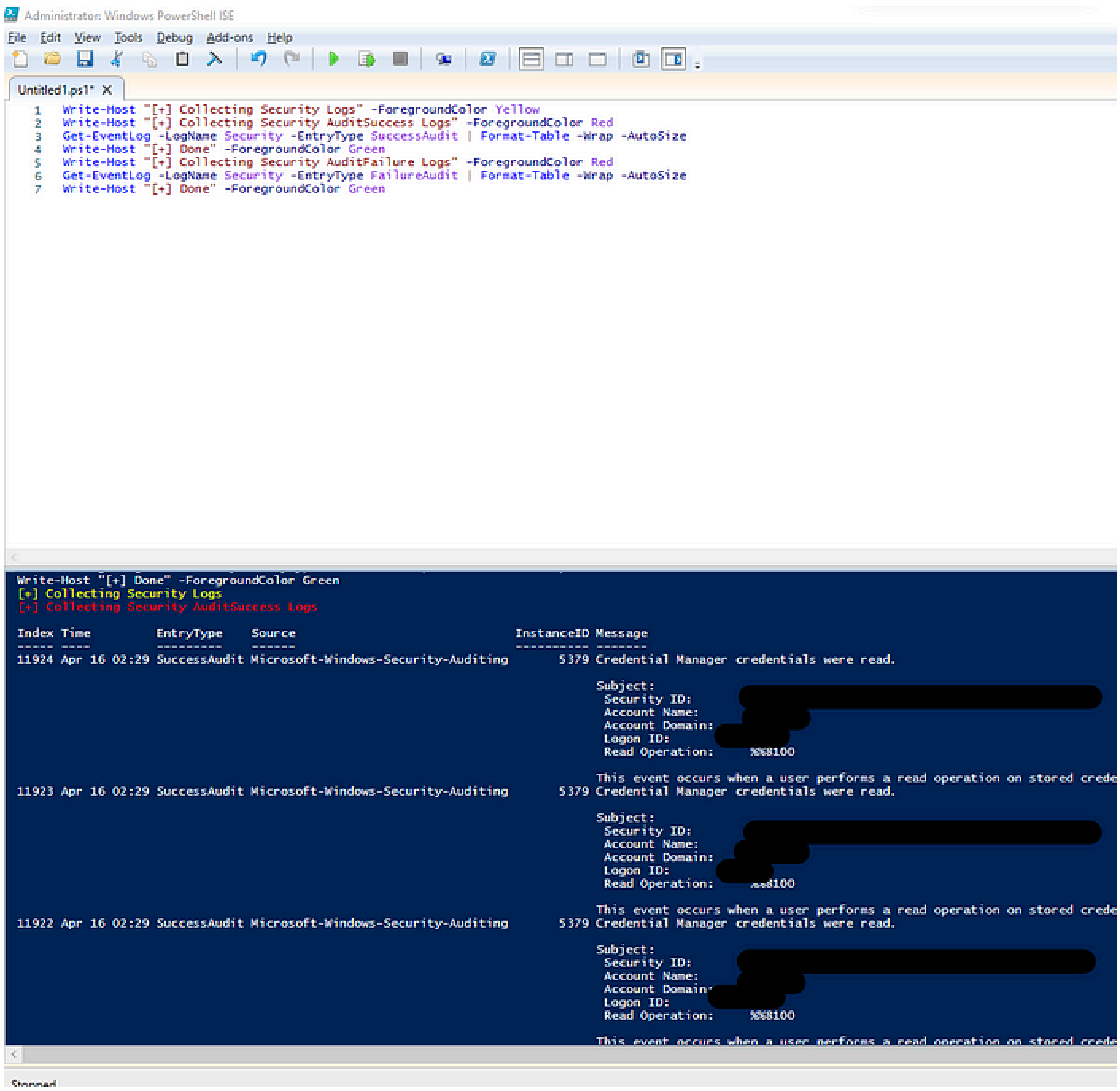
```
Get-EventLog -LogName Security | Format-Table -Wrap -AutoSize
```



```
PS D:\> Get-EventLog -LogName Security | Format-Table -Wrap -AutoSize

Index Time         EntryType    Source                                  InstanceID Message
----- ----         ---------    ------                                  ---------- -------
11897 Apr 16 02:04 SuccessAudit Microsoft-Windows-Security-Auditing           4672 Special privileges assigned to new logon.

                                                                                   Subject:
                                                                                    Security ID:          [redacted]

                                                                                    Account Name:         SYSTEM

                                                                                    Account Domain:       NT AUTHORITY

                                                                                    Logon ID:             [redacted]

                                                                                   Privileges:            SeAssignPrimaryTokenPrivilege
                                                                                                  SeTcbPrivilege
                                                                                                  SeSecurityPrivilege
                                                                                                  SeTakeOwnershipPrivilege
                                                                                                  SeLoadDriverPrivilege
                                                                                                  SeBackupPrivilege
                                                                                                  SeRestorePrivilege
                                                                                                  SeDebugPrivilege
                                                                                                  SeAuditPrivilege
                                                                                                  SeSystemEnvironmentPrivilege
                                                                                                  SeImpersonatePrivilege
                                                                                                  SeDelegateSessionUserImpersonatePrivilege
11896 Apr 16 02:04 SuccessAudit Microsoft-Windows-Security-Auditing           4624 An account was successfully logged on.

                                                                                   Subject:
                                                                                    Security ID:          [redacted]

                                                                                    Account Name:         [redacted]

                                                                                    Account Domain:       WORKGROUP

                                                                                    Logon ID:             [redacted]

                                                                                   Logon Information:
                                                                                    Logon Type:           5

                                                                                    Restricted Admin Mode: -
                                                                                    Virtual Account:      [redacted]

                                                                                    Elevated Token:       [redacted]

                                                                                   Impersonation Level:   [redacted]

                                                                                   New Logon:
                                                                                    Security ID:          [redacted]
```

In Security Logs you can find two entry types, "SuccessAudit" and "FailureAudit". Paste the following line of codes in your Powershell ISE for capturing the System Logs.

```
Write-Host "Collecting Security Logs" -ForegroundColor Yellow
Write-Host "Collecting Security AuditSuccess Logs" -ForegroundColor Red

Get-EventLog -LogName Security -EntryType SuccessAudit | Format-Table -Wrap -AutoSize

Write-Host "Done" -ForegroundColor Green
Write-Host "Collecting Security AuditFailure Logs" -ForegroundColor Red

Get-EventLog -LogName Security -EntryType FailureAudit | Format-Table -Wrap -AutoSize

Write-Host "Done" -ForegroundColor Green
```


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*
Stopped

```
Write-Host "[+] Collecting Security Logs" -ForegroundColor Yellow
Write-Host "[+] Collecting Security AuditSuccess Logs" -ForegroundColor Red
Get-EventLog -LogName Security -EntryType SuccessAudit | Format-Table -Wrap -AutoSize
Write-Host "[+] Done" -ForegroundColor Green
Write-Host "[+] Collecting Security AuditFailure Logs" -ForegroundColor Red
Get-EventLog -LogName Security -EntryType FailureAudit | Format-Table -Wrap -AutoSize
Write-Host "[+] Done" -ForegroundColor Green
```

```
Write-Host "[+] Done" -ForegroundColor Green
[+] Collecting Security Logs
[+] Collecting Security AuditSuccess Logs

Index Time          EntryType    Source                                  InstanceID Message
----- ----          ---------    ------                                  ---------- -------
11924 Apr 16 02:29 SuccessAudit Microsoft-Windows-Security-Auditing          5379 Credential Manager credentials were read.

                                                                                  Subject:
                                                                                   Security ID:      [redacted]
                                                                                   Account Name:
                                                                                   Account Domain:
                                                                                   Logon ID:
                                                                                   Read Operation:      %%8100

                                                                                  This event occurs when a user performs a read operation on stored crede
11923 Apr 16 02:29 SuccessAudit Microsoft-Windows-Security-Auditing          5379 Credential Manager credentials were read.

                                                                                  Subject:
                                                                                   Security ID:      [redacted]
                                                                                   Account Name:
                                                                                   Account Domain:
                                                                                   Logon ID:
                                                                                   Read Operation:      %%8100

                                                                                  This event occurs when a user performs a read operation on stored crede
11922 Apr 16 02:29 SuccessAudit Microsoft-Windows-Security-Auditing          5379 Credential Manager credentials were read.

                                                                                  Subject:
                                                                                   Security ID:      [redacted]
                                                                                   Account Name:
                                                                                   Account Domain:
                                                                                   Logon ID:
                                                                                   Read Operation:      %%8100

                                                                                  This event occurs when a user performs a read operation on stored crede
```

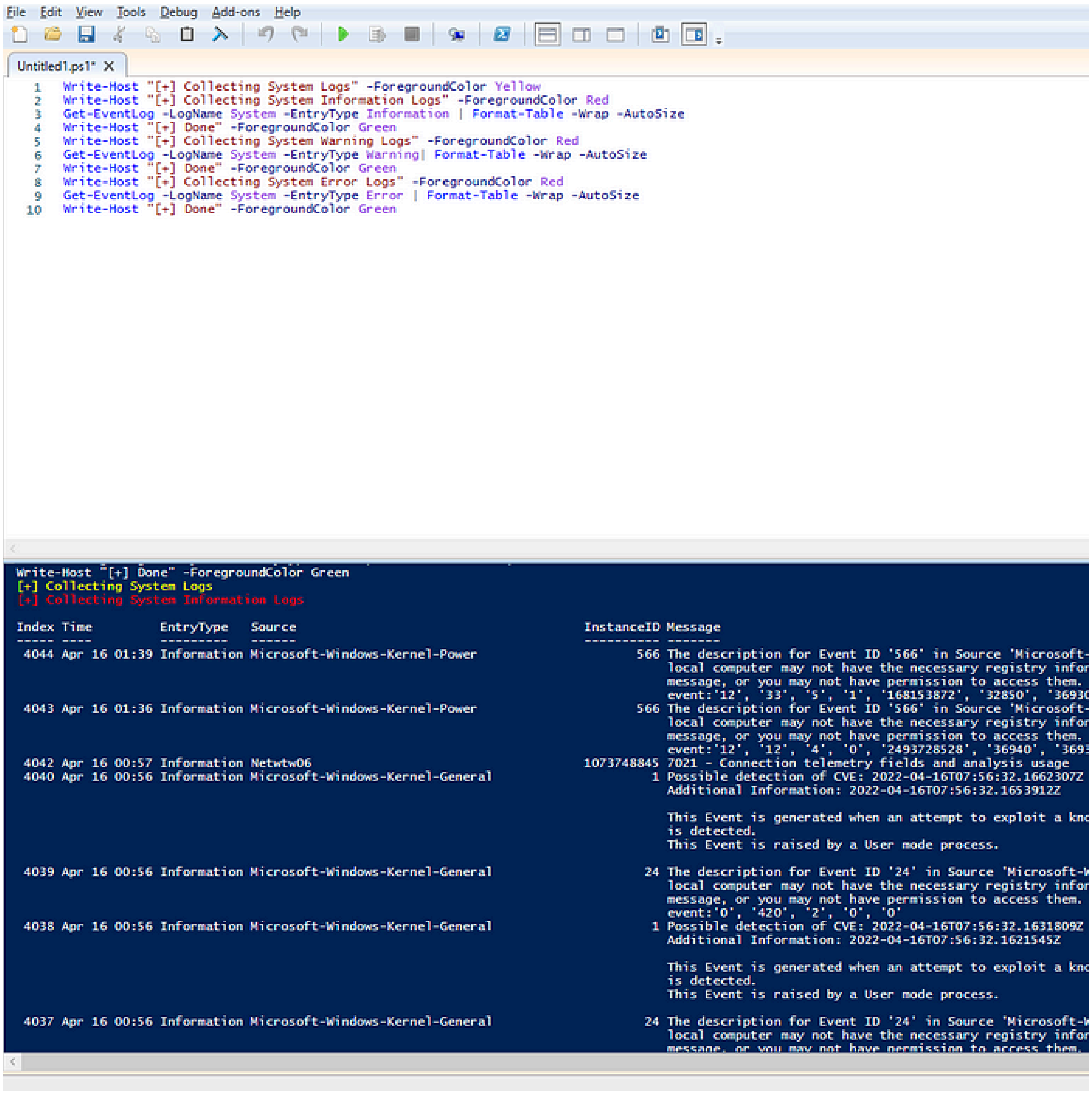
3.4. System Logs Parsing

EntryType for Application and System Logs are same. System Logs comprises of three EntryTypes "Information,Warning & Error".

Because the syntax of System Logs is the same as above two, you can paste the following line of codes in Powershell ISE to generate the System Logs based on EventType.

```
Write-Host "Collecting System Logs" -ForegroundColor Yellow
Write-Host "Collecting System Information Logs" -ForegroundColor Red

Get-EventLog -LogName System -EntryType Information | Format-Table -Wrap -AutoSize

Write-Host "Done" -ForegroundColor Green
Write-Host "Collecting System Warning Logs" -ForegroundColor Red

Get-EventLog -LogName System -EntryType Warning| Format-Table -Wrap -AutoSize
```

```
Write-Host "Done" -ForegroundColor Green
Write-Host "Collecting System Error Logs" -ForegroundColor Red

Get-EventLog -LogName System -EntryType Error | Format-Table -Wrap -AutoSize

Write-Host "Done" -ForegroundColor Green
```



```
Write-Host "[+] Collecting System Logs" -ForegroundColor Yellow
Write-Host "[+] Collecting System Information Logs" -ForegroundColor Red
Get-EventLog -LogName System -EntryType Information | Format-Table -Wrap -AutoSize
Write-Host "[+] Done" -ForegroundColor Green
Write-Host "[+] Collecting System Warning Logs" -ForegroundColor Red
Get-EventLog -LogName System -EntryType Warning| Format-Table -Wrap -AutoSize
Write-Host "[+] Done" -ForegroundColor Green
Write-Host "[+] Collecting System Error Logs" -ForegroundColor Red
Get-EventLog -LogName System -EntryType Error | Format-Table -Wrap -AutoSize
Write-Host "[+] Done" -ForegroundColor Green
```

```
Write-Host "[+] Done" -ForegroundColor Green
[+] Collecting System Logs
[+] Collecting System Information Logs

Index Time          EntryType   Source                                  InstanceID Message
----- ----          ---------   ------                                  ---------- -------
 4044 Apr 16 01:39 Information Microsoft-Windows-Kernel-Power                  566 The description for Event ID '566' in Source 'Microsoft-
                                                                                   local computer may not have the necessary registry infor
                                                                                   message, or you may not have permission to access them.
                                                                                   event:'12', '33', '5', '1', '168153872', '32850', '3693
 4043 Apr 16 01:36 Information Microsoft-Windows-Kernel-Power                  566 The description for Event ID '566' in Source 'Microsoft-
                                                                                   local computer may not have the necessary registry infor
                                                                                   message, or you may not have permission to access them.
                                                                                   event:'12', '12', '4', '0', '2493728528', '36940', '369
 4042 Apr 16 00:57 Information Netwtw06                                 1073748845 7021 - Connection telemetry fields and analysis usage
 4040 Apr 16 00:56 Information Microsoft-Windows-Kernel-General                  1 Possible detection of CVE: 2022-04-16T07:56:32.1662307Z
                                                                                   Additional Information: 2022-04-16T07:56:32.1653912Z

                                                                                   This Event is generated when an attempt to exploit a kno
                                                                                   is detected.
                                                                                   This Event is raised by a User mode process.

 4039 Apr 16 00:56 Information Microsoft-Windows-Kernel-General                 24 The description for Event ID '24' in Source 'Microsoft-W
                                                                                   local computer may not have the necessary registry infor
                                                                                   message, or you may not have permission to access them.
                                                                                   event:'0', '420', '2', '0', '0'
 4038 Apr 16 00:56 Information Microsoft-Windows-Kernel-General                  1 Possible detection of CVE: 2022-04-16T07:56:32.1631809Z
                                                                                   Additional Information: 2022-04-16T07:56:32.1621545Z

                                                                                   This Event is generated when an attempt to exploit a kno
                                                                                   is detected.
                                                                                   This Event is raised by a User mode process.

 4037 Apr 16 00:56 Information Microsoft-Windows-Kernel-General                 24 The description for Event ID '24' in Source 'Microsoft-W
                                                                                   local computer may not have the necessary registry infor
                                                                                   message, or you may not have permission to access them.
```

3.5. What would be Advanced Logs Parsing with Powershell?

So far, we have discussed about parsing the major EventLogs of the Windows system. But as mentioned in the screenshot of the \winevt\Logs directory, there is a list of Logs generated by Windows system. How can we parse those Log files?

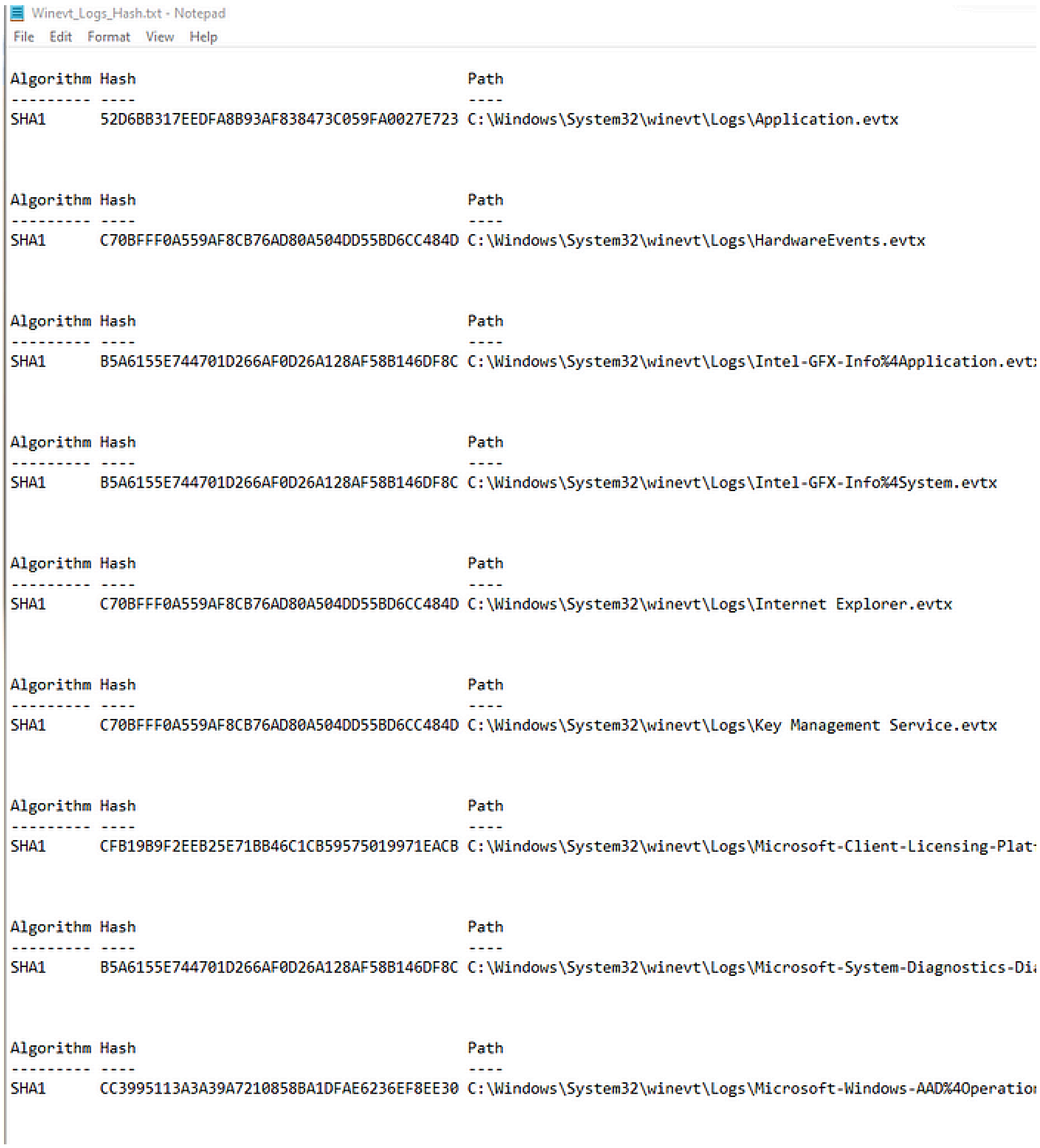
A better idea would be copying those .evtx files in your External drive and parse those .evtx files in your Lab system. However, wouldn't copying these .evtx files tamper with the integrity of these files?

As a result, Powershell helps us once again by enabling us to create Hashes of all the .evtx files before copying them. And after copying these files, we can verify the integrity of these files.

You can create Hashes of all the files in one go by pasting the code in the Powershell ISE window, and you need to wait for a while since there are a large number of files so it will take a minute or else depends upon the system computation power.

```
Get-ChildItem 'C:\Windows\System32\winevt\Logs\' -File -Recurse -PipelineVariable
File | ForEach-Object {
    $stream = try {
        [IO.FileStream]::new($File.FullName, [IO.FileMode]::Open,
[IO.FileAccess]::Read, [IO.FileShare]::Read)
    }
    catch {
        [IO.FileStream]::new( $File.FullName, [IO.FileMode]::Open,
[IO.FileAccess]::Read, [IO.FileShare]::ReadWrite )
    }

    if( $stream ) {
        try {
            Get-FileHash -InputStream $stream -Algorithm SHA1 |
                Select-Object Algorithm, Hash, @{ Name = 'Path'; Expression = {
$File.Fullname } } | Format-Table -Wrap -AutoSize >> <Path\_To\_Hash\_File.txt>
        }
        finally {
            $stream.Close()
        }
    }
}
```

> *To understand the code, you may refer to the below provided link:*
>
> https://stackoverflow.com/questions/58466227/get-filehash-unable-to-read-the-file



```
Algorithm Hash                                     Path
--------- ----                                     ----
SHA1      52D6BB317EEDFA8B93AF838473C059FA0027E723 C:\Windows\System32\winevt\Logs\Application.evtx


Algorithm Hash                                     Path
--------- ----                                     ----
SHA1      C70BFFF0A559AF8CB76AD80A504DD55BD6CC484D C:\Windows\System32\winevt\Logs\HardwareEvents.evtx


Algorithm Hash                                     Path
--------- ----                                     ----
SHA1      B5A6155E744701D266AF0D26A128AF58B146DF8C C:\Windows\System32\winevt\Logs\Intel-GFX-Info%4Application.evt


Algorithm Hash                                     Path
--------- ----                                     ----
SHA1      B5A6155E744701D266AF0D26A128AF58B146DF8C C:\Windows\System32\winevt\Logs\Intel-GFX-Info%4System.evtx


Algorithm Hash                                     Path
--------- ----                                     ----
SHA1      C70BFFF0A559AF8CB76AD80A504DD55BD6CC484D C:\Windows\System32\winevt\Logs\Internet Explorer.evtx


Algorithm Hash                                     Path
--------- ----                                     ----
SHA1      C70BFFF0A559AF8CB76AD80A504DD55BD6CC484D C:\Windows\System32\winevt\Logs\Key Management Service.evtx


Algorithm Hash                                     Path
--------- ----                                     ----
SHA1      CFB19B9F2EEB25E71BB46C1CB59575019971EACB C:\Windows\System32\winevt\Logs\Microsoft-Client-Licensing-Plat-


Algorithm Hash                                     Path
--------- ----                                     ----
SHA1      B5A6155E744701D266AF0D26A128AF58B146DF8C C:\Windows\System32\winevt\Logs\Microsoft-System-Diagnostics-Di


Algorithm Hash                                     Path
--------- ----                                     ----
SHA1      CC3995113A3A39A7210858BA1DFAE6236EF8EE30 C:\Windows\System32\winevt\Logs\Microsoft-Windows-AAD%4Operatio
```

Once our hashes of all the .evtx files from the /winevt/Logs directory are ready, we can recursively copy each of the files from the directory to the specified path. For that, paste the following code in Powershell ISE

```
Write-Host "Enter Path to save Log Files: " -ForegroundColor Yellow
Write-Host "Path Syntax: Drive:\Folder\" -ForegroundColor Cyan

$path = Read-Host

ls -Path C:\Windows\System32\winevt\Logs\ -File -Recurse |
    Where-Object {$_.Extension -eq ".evtx"} |
    ForEach-Object {
        cp $_.FullName -Destination $path
    }
```

> **Note:** Make sure the drive is empty and specify directory in proper format where you want to save the Log files as this is going to feed 100+ .evtx files in that directory.

With use of above command, we have stored all the Log files inside our defined directory. As an investigator, we are not going to manually check all the files and examine the logs. To ease with this task, Powershell provides us with recursive function to convert each of .evtx file into a HTML file and at last, we can create an Index Page for all the log files.

But, we can view the content of any .evtx file using the following command

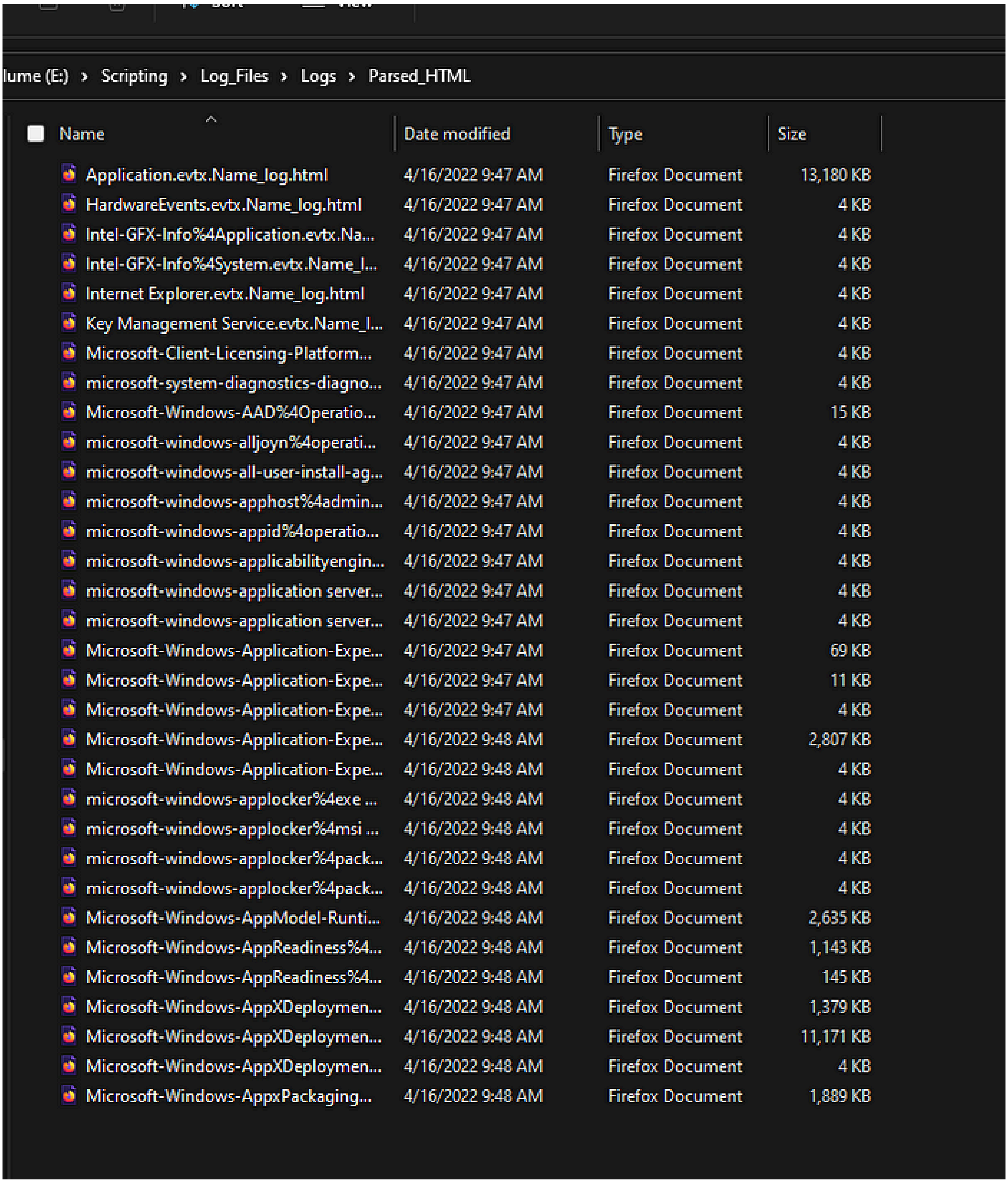
```
Get-WinEvent -Path <Name\_of\_evtx\_file.evtx>
```

Now lets convert all the .evtx files to .html files. For this, paste the following lines of code in Powershell ISE.

```
Write-Host "Converting .evtx to .html" -ForegroundColor DarkYellow
Write-Host ""

Write-Host "Enter path for the copied Logs folder (For eg, C:\..\..\)"
$path = Read-Host
Write-Host ""

Write-Host "Enter path to save the .html files (For eg, C:\..\..\)"
$outputpath = Read-Host
Write-Host ""

ls -Path $path -File |
    Where-Object {$_.Extension -eq ".evtx"} |
    ForEach-Object {
        Write-Host "Converting file: $_" -ForegroundColor Red
        $name = $_.Name
        $file = "$_.Name" + "_log.html"
        $outputfile = $outputpath + $file
        $log2html = (Get-WinEvent -Path $_.PsPath | ConvertTo-Html | Out-File -
FilePath $outputfile)
    }

Write-Host "Done" -ForegroundColor Green
```

Note: Do not worry if you see any error while converting evtx to html. The error is generated for those files which do not contain any Log entry

After running this in Powershell ISE, the output directory must have the parsed HTML files of the .evtx files as displayed in the below screenshot.


lume (E:) › Scripting › Log_Files › Logs › Parsed_HTML

Name	Date modified	Type	Size
Application.evtx.Name_log.html	4/16/2022 9:47 AM	Firefox Document	13,180 KB
HardwareEvents.evtx.Name_log.html	4/16/2022 9:47 AM	Firefox Document	4 KB
Intel-GFX-Info%4Application.evtx.Na...	4/16/2022 9:47 AM	Firefox Document	4 KB
Intel-GFX-Info%4System.evtx.Name_l...	4/16/2022 9:47 AM	Firefox Document	4 KB
Internet Explorer.evtx.Name_log.html	4/16/2022 9:47 AM	Firefox Document	4 KB
Key Management Service.evtx.Name_l...	4/16/2022 9:47 AM	Firefox Document	4 KB
Microsoft-Client-Licensing-Platform...	4/16/2022 9:47 AM	Firefox Document	4 KB
microsoft-system-diagnostics-diagno...	4/16/2022 9:47 AM	Firefox Document	4 KB
Microsoft-Windows-AAD%4Operatio...	4/16/2022 9:47 AM	Firefox Document	15 KB
microsoft-windows-alljoyn%4operati...	4/16/2022 9:47 AM	Firefox Document	4 KB
microsoft-windows-all-user-install-ag...	4/16/2022 9:47 AM	Firefox Document	4 KB
microsoft-windows-apphost%4admin...	4/16/2022 9:47 AM	Firefox Document	4 KB
microsoft-windows-appid%4operatio...	4/16/2022 9:47 AM	Firefox Document	4 KB
microsoft-windows-applicabilityengin...	4/16/2022 9:47 AM	Firefox Document	4 KB
microsoft-windows-application server...	4/16/2022 9:47 AM	Firefox Document	4 KB
microsoft-windows-application server...	4/16/2022 9:47 AM	Firefox Document	4 KB
Microsoft-Windows-Application-Expe...	4/16/2022 9:47 AM	Firefox Document	69 KB
Microsoft-Windows-Application-Expe...	4/16/2022 9:47 AM	Firefox Document	11 KB
Microsoft-Windows-Application-Expe...	4/16/2022 9:47 AM	Firefox Document	4 KB
Microsoft-Windows-Application-Expe...	4/16/2022 9:48 AM	Firefox Document	2,807 KB
Microsoft-Windows-Application-Expe...	4/16/2022 9:48 AM	Firefox Document	4 KB
microsoft-windows-applocker%4exe ...	4/16/2022 9:48 AM	Firefox Document	4 KB
microsoft-windows-applocker%4msi ...	4/16/2022 9:48 AM	Firefox Document	4 KB
microsoft-windows-applocker%4pack...	4/16/2022 9:48 AM	Firefox Document	4 KB
microsoft-windows-applocker%4pack...	4/16/2022 9:48 AM	Firefox Document	4 KB
Microsoft-Windows-AppModel-Runti...	4/16/2022 9:48 AM	Firefox Document	2,635 KB
Microsoft-Windows-AppReadiness%4...	4/16/2022 9:48 AM	Firefox Document	1,143 KB
Microsoft-Windows-AppReadiness%4...	4/16/2022 9:48 AM	Firefox Document	145 KB
Microsoft-Windows-AppXDeploymen...	4/16/2022 9:48 AM	Firefox Document	1,379 KB
Microsoft-Windows-AppXDeploymen...	4/16/2022 9:48 AM	Firefox Document	11,171 KB
Microsoft-Windows-AppXDeploymen...	4/16/2022 9:48 AM	Firefox Document	4 KB
Microsoft-Windows-AppxPackaging...	4/16/2022 9:48 AM	Firefox Document	1,889 KB

4. Where's the Report?

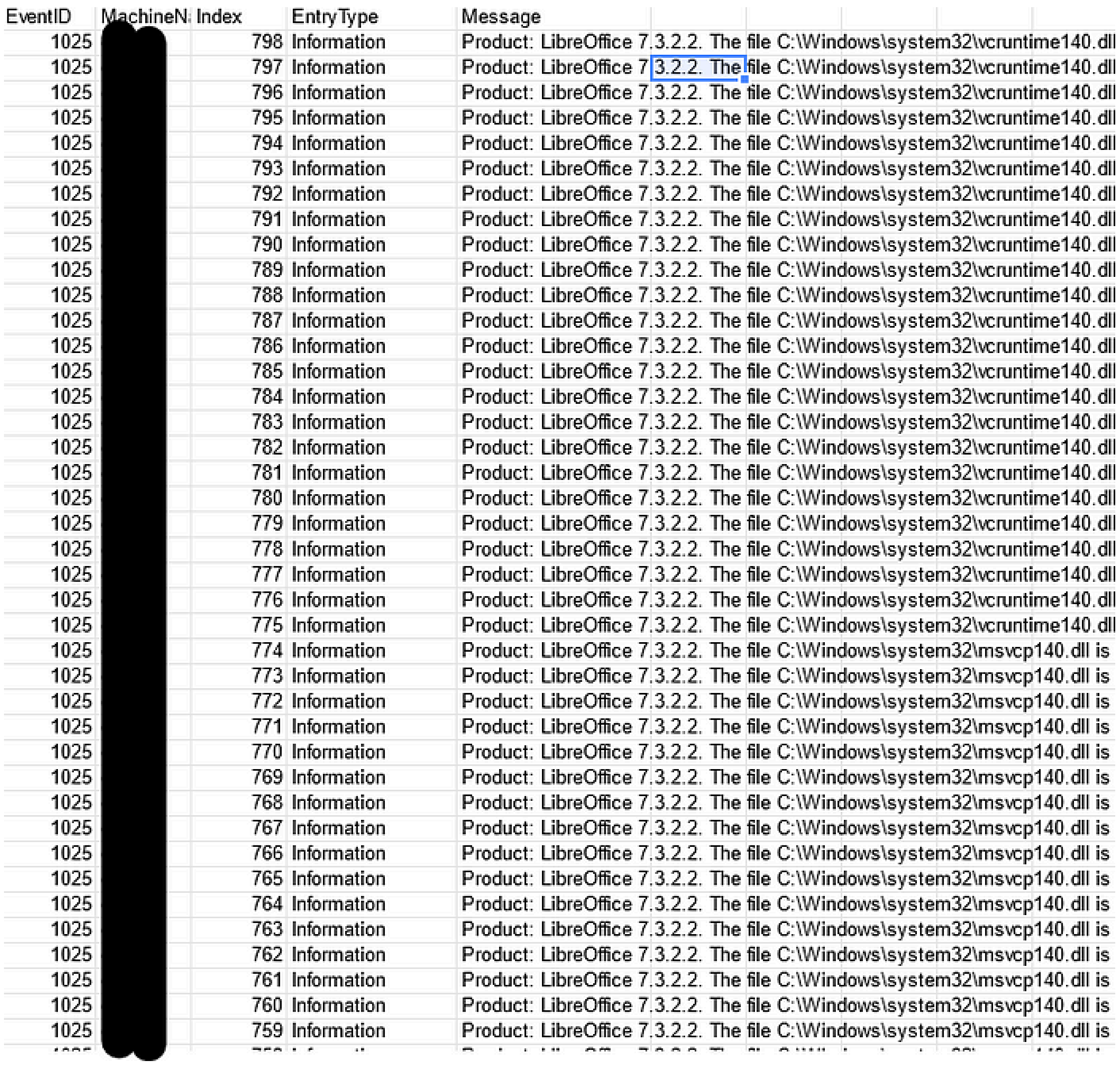
Powershell provides us with the capability to save our output in HTML, CSV or XML format. The major focus of this blog will be to create a HTML report with custom CSS, but we will also discuss how to create a CSV file out of the output.

Paste the following command within the Powershell window to generate a CSV file of the output.

> Get-EventLog -LogName Application -EntryType Information | Select-Object EventID,MachineName,Index,EntryType,Message | Export-Csv -Path <Path.csv> -NoTypeInformation -

> NoClobber

This will create a CSV file for the Application logs with EntryType Information. Output of the CSV file is displayed below.



EventID	MachineN	Index	EntryType	Message
1025	[redacted]	798	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	797	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	796	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	795	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	794	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	793	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	792	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	791	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	790	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	789	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	788	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	787	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	786	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	785	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	784	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	783	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	782	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	781	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	780	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	779	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	778	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	777	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	776	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	775	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\vcruntime140.dll
1025	[redacted]	774	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	773	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	772	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	771	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	770	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	769	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	768	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	767	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	766	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	765	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	764	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	763	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	762	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	761	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	760	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is
1025	[redacted]	759	Information	Product: LibreOffice 7.3.2.2. The file C:\Windows\system32\msvcp140.dll is

Similarly, we can create CSV for any type of Log when running any of the above command and piping with Export-Csv cmdlet.

Moving further, now we have to create Index page for our large number of parsed HTML files. The Index page would tell about the FileName, FileSize and Location of the file with link to open the file from the Index page itself.

Before creating the Index page, we have to rename some of the html files cause the file name consists of special character like "%4" which when added to html file as "Location Link", it is changed to Unicode character which will create error in our Index Page. So, to remove this "%4", run the following code in Powershell

```
Write-Host "Enter path for the parsed HTML Logs directory: "
$path= Read-Host
```

```
Get-ChildItem $path -Recurse |
    Where-Object { $_.Extension -eq '.html' } |
    Where-Object { $_.Name -match '%4' } |
    Rename-Item -NewName { $_.Name -replace '%4','' }
```

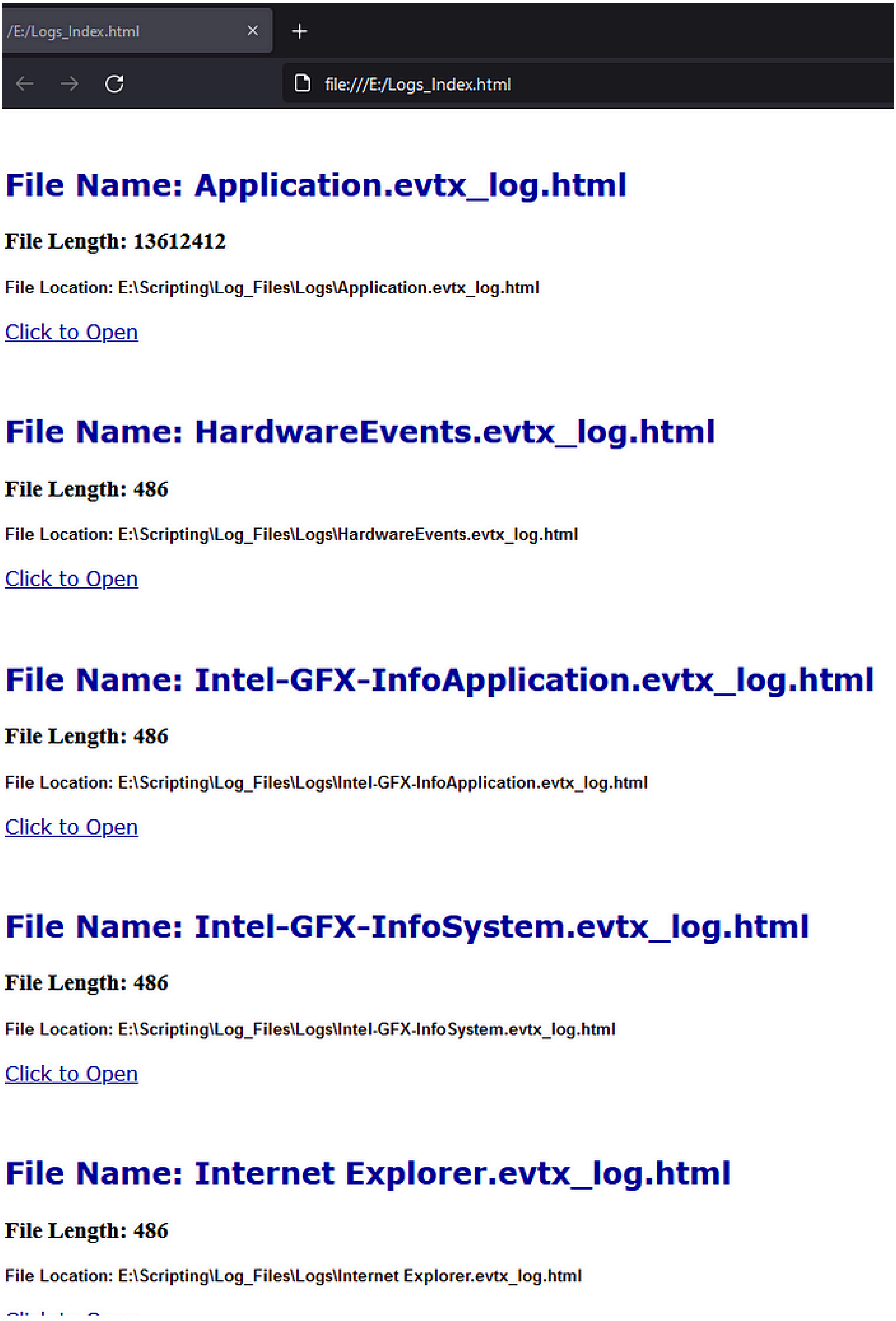
As the special character is removed from our parsed html files name, now we are good to go to create our Index page. Paste the below code in Powershell ISE to generate the Index page

```
$header = @"
<style>
    body{
        background-color: #ffffff;
    }
    h1 {
        font-family: Verdana, Helvetica, sans-serif;
        color: black;
        font-size: 28px;
    }
    h2 {
        font-family: Verdana, Helvetica, sans-serif;
        color: #000099;
    }
    a{
        font-family: Verdana, Helvetica, sans-serif;
        color: #000099;
    }
    td{
        font-family: "Verdana", "Helvetica Neue", Helvetica, Arial, sans-sertd;
        color: rgb(17,1,1);
    }
    h4{
        font-family: "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;
        color: rgb(17, 1, 1);
        font-size: small;
    }
    iframe{
        border:none;
        width:100%;
        height:100%;
        display:block;
    }
    .marginauto {
        margin: 10px auto 20px;
        display: block;
    }
    p{
        font-family: Verdana, Helvetica, sans-serif;
        color: black;
    }
    .center {
        display: block;
```

```
            margin-left: auto;
            margin-right: auto;
            width: 50%;
        }
        .styled-table{
            border-collapse: collapse;
            margin: 25px 0;
            font-size: 0.9em;
            font-family: Verdana, Geneva, Tahoma, sans-serif;
            min-width: 400px;
            box-shadow: 0 0 20px rgba(0, 0, 0, 0.15);
        }
        .styled-table thead tr {
            background-color: #009879;
            color: #ffffff;
            text-align: left;
        }
        .styled-table th,
        .styled-table td {
            padding: 12px 15px;
        }
        .styled-table tbody tr {
            border-bottom: 1px solid #dddddd;
        }

        .styled-table tbody tr:nth-of-type(even) {
            background-color: #f3f3f3;
        }

        .styled-table tbody tr:last-of-type {
            border-bottom: 2px solid #009879;
        }
    </style
    "@

    function New-Reporter {
        [CmdletBinding()]
        param (
            [Parameter()]
            [String] $ParameterName,
            [Parameter()]
            [String] $location,
            [Parameter()]
            [String] $length
        )

        $heading = @"
        <br>
        <div>
            <h2>File Name: $File</h2>
            <h3>File Length: $length</h3>
            <h4>File Location: $location</h4>
            <a href='$location'>Click to Open</a>
        </div>
        <br>
    "@

        $Global:report += ($heading)
    }

    function New-Indexer {
        [CmdletBinding()]
        param (

        )

        Get-ChildItem $path -File -Recurse -PipelineVariable File |
            Where-Object { $_.Extension -eq '.html' } |
            ForEach-Object {
                $stream = try {
                    [IO.FileStream]::new($File.FullName, [IO.FileMode]::Open,
    [IO.FileAccess]::Read, [IO.FileShare]::Read)
                }
                catch {
                    [IO.FileStream]::new($File.FullName, [IO.FileMode]::Open,
    [IO.FileAccess]::Read, [IO.FileShare]::ReadWrite)
                }
                if ($stream) {
                    try {
                        $location = $File.FullName
                        $length = $File.Length
                        New-Reporter $File $location $length
                    }
                    finally {
                        $stream.Close()
                    }
                }
            }
    }

    function Invoke-TroubleShootingReport {
        [CmdletBinding()]
        param (
            [Parameter()]
            [String] $Path
        )

        Write-Host "Write Path for the Saved Logs HTML Files (Format: C:\..\)"
        $Global:path = Read-Host

        Write-Host "Write Path for Index Page: "
        $indexpath = Read-Host

        New-Indexer

        $outputreport = $indexpath + "Logs_Index.html"
        ConvertTo-Html -Head $header -Body $report -Title LOGS_INDEX | Out-File
    $outputreport
```

```
}

Invoke-TroubleShootingReport

$Global:report = New-Reporter @()
```

Output for the above code would result in creating an Index page, with Name of the HTML file, Size of the HTML file and Location of the HTML file to directly open the file from the Index page. The output should result as displayed in the below screenshot



File Name: Application.evtx_log.html

File Length: 13612412

File Location: E:\Scripting\Log_Files\Logs\Application.evtx_log.html

Click to Open

File Name: HardwareEvents.evtx_log.html

File Length: 486

File Location: E:\Scripting\Log_Files\Logs\HardwareEvents.evtx_log.html

Click to Open

File Name: Intel-GFX-InfoApplication.evtx_log.html

File Length: 486

File Location: E:\Scripting\Log_Files\Logs\Intel-GFX-InfoApplication.evtx_log.html

Click to Open

File Name: Intel-GFX-InfoSystem.evtx_log.html

File Length: 486

File Location: E:\Scripting\Log_Files\Logs\Intel-GFX-InfoSystem.evtx_log.html

Click to Open

File Name: Internet Explorer.evtx_log.html

File Length: 486

File Location: E:\Scripting\Log_Files\Logs\Internet Explorer.evtx_log.html

Click to Open

As seen in the above screenshot, the index page would contain the FileName, FileLength, FileLocation and Link to open the file.

Important thing to mention is there would be some files that won't open as there's no entry inside them. The reason for including all the .evtx files within this Index Page is that for different users there will be different kinds of entries, so as investigators, we cannot ignore any single Log file.

So, if you go to Index Page and click on link for Application.evtx_log.html, this would open the Application Logs for the system.

Any viewer can modify the code as per the usability and can use this in their investigation procedures.

> **Note:** *Whenever you type the directory name, always end the directory with '\', otherwise the output path may differ. For e.g, if you want to save your files in any folder within D: directory, type 'D:\directory_name\'*

5. Conclusion

As mentioned in the beginning, Windows Event Logs are one of the most important artifacts when investigating any Windows system. A thorough investigation should not restrict itself to just the major Events like Application, Security and System, but should also examine other Event Logs present in the system. These other Log files might contain some useful information that will assist the investigator in their analysis.

As part of the Windows Triaging with Powershell, the next step is to gather the important artifacts from Live Windows System with Powershell and to generate a report along with all the collected artifacts' hashes.

Until then, any comments or suggestions on this would be greatly appreciated to create some new content for the readers.