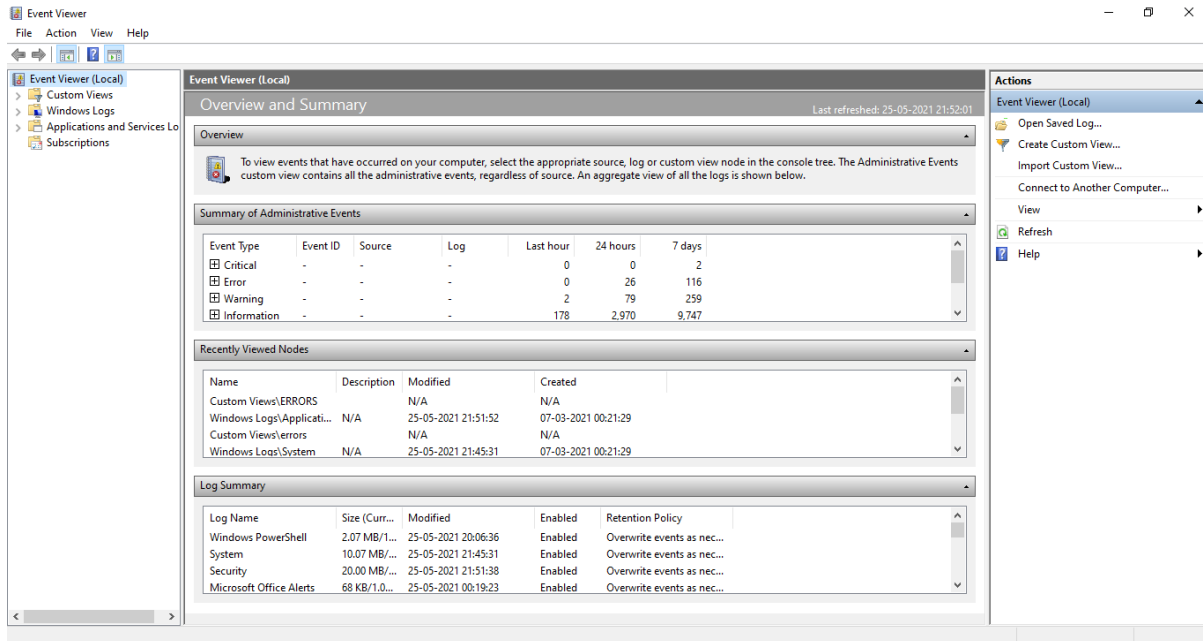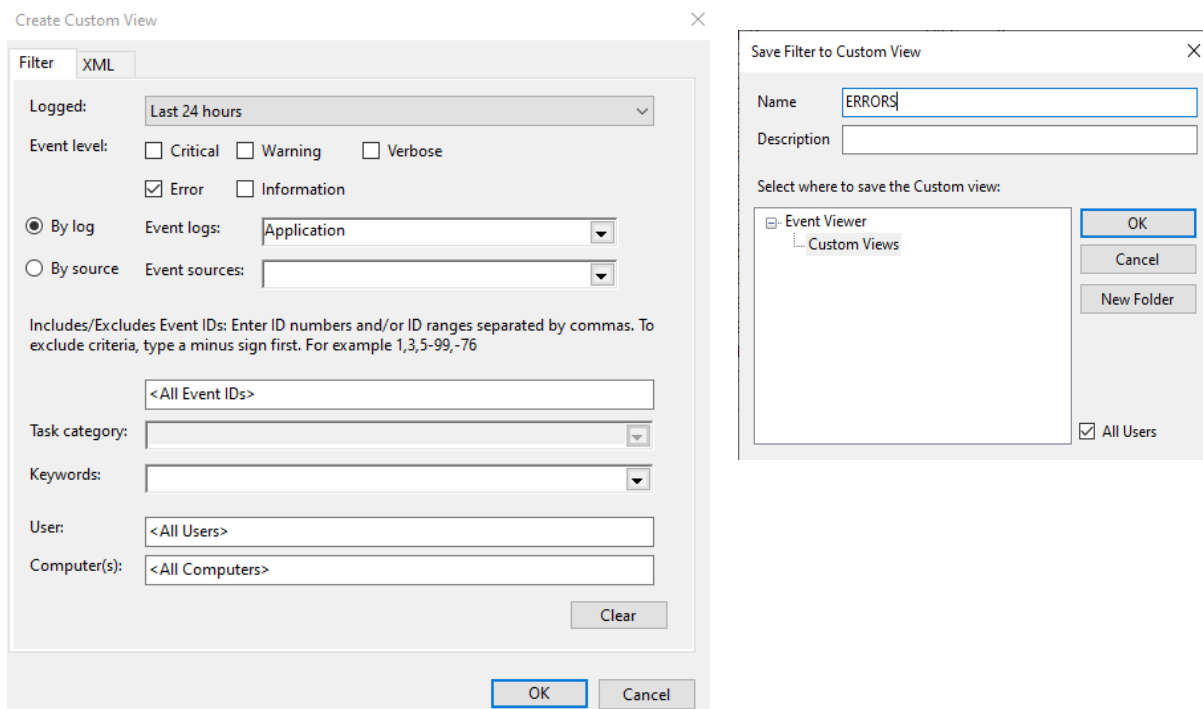# MODULE 2 : Operating Systems and You (WEEK 6 ASSIGNMENT)
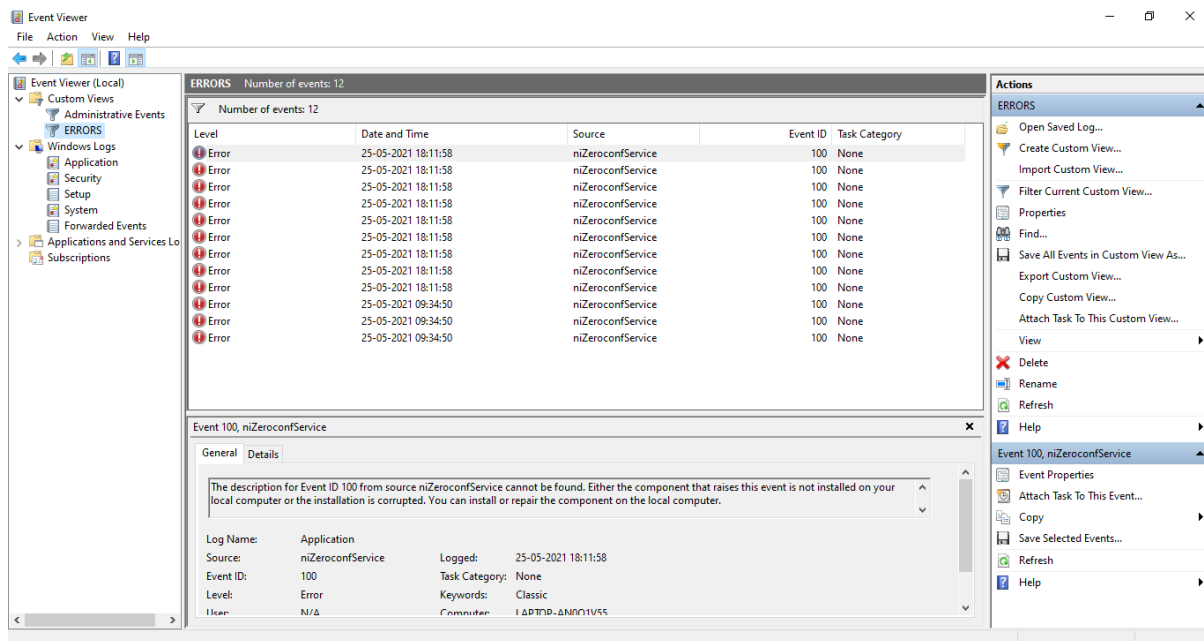
Accessing Windows Event Viewer for Logs

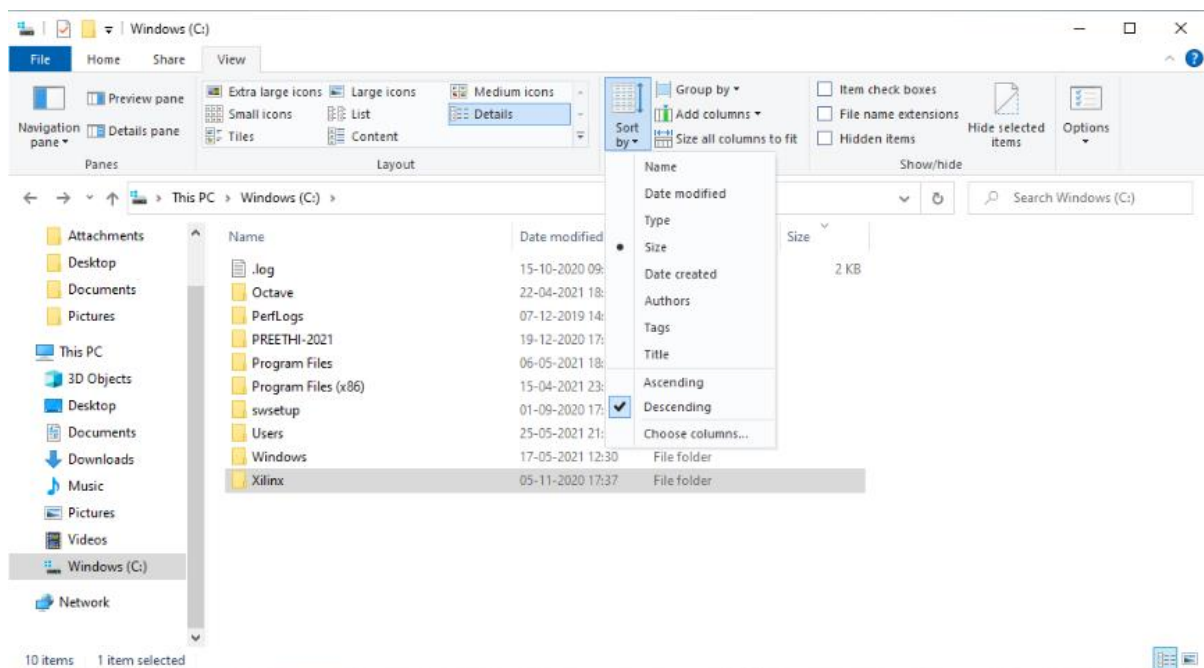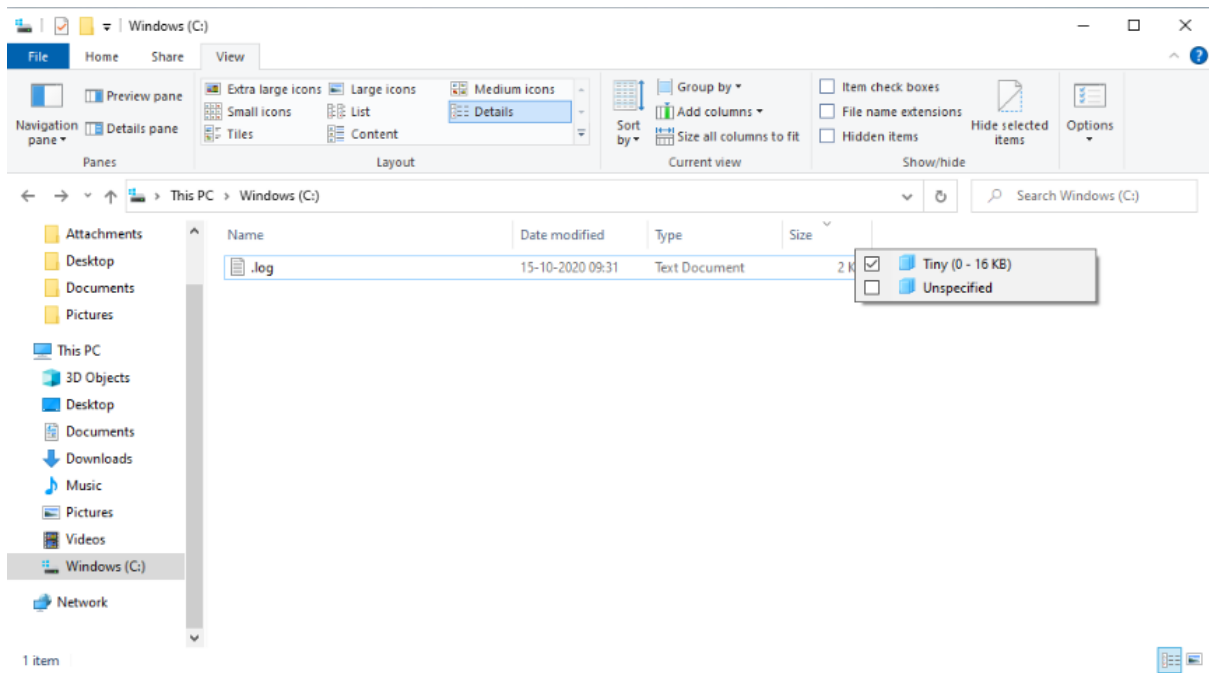## Extracting Error logs in Event Viewer

Error logs

For the assignment, there are five different issues that we need to resolve, using the skills we've learned so far in this course. But, solving these error logs shown here is out of scope for this assignment. Thus, below are few demonstrations of the skills I've picked up from this course.

Viewing folders based on Size

Creating and removing Folders from CLI


```
PS C:\Users\rishi\Documents\RISHIKA> cd C:\users
PS C:\users> mkdir newfolder


    Directory: C:\users


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        25-05-2021     21:11               newfolder


PS C:\users> ls


    Directory: C:\users


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        25-05-2021     21:11               newfolder
d-r---        07-03-2021     13:45               Public
d-----        15-05-2021     19:36               rishi


PS C:\users> rm newfolder
PS C:\users> ls


    Directory: C:\users


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        07-03-2021     13:45               Public
d-----        15-05-2021     19:36               rishi
```

Viewing Permissions of a file

```
Administrator: Windows PowerShell
PS C:\Users\rishi\Documents\RISHIKA\extra\python(UMich)> icacls words.txt
words.txt LAPTOP-AN0O1V55\rishi:(R)
          NT AUTHORITY\SYSTEM:(I)(F)
          BUILTIN\Administrators:(I)(F)
          LAPTOP-AN0O1V55\rishi:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

Granting Permissions to different users

```
PS C:\Users\rishi\Documents\RISHIKA\extra\python(UMich)> icacls words.txt /grant "rishi:(w)"
processed file: words.txt
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\rishi\Documents\RISHIKA\extra\python(UMich)> icacls words.txt /grant "Everyone:(x)"
processed file: words.txt
Successfully processed 1 files; Failed processing 0 files
```

```
PS C:\Users\rishi\Documents\RISHIKA\extra\python(UMich)> icacls words.txt
words.txt Everyone:(X)
          LAPTOP-AN0O1V55\rishi:(R,W)
          NT AUTHORITY\SYSTEM:(I)(F)
          BUILTIN\Administrators:(I)(F)
          LAPTOP-AN0O1V55\rishi:(I)(F)
```

Removing Permissions

```
PS C:\Users\rishi\Documents\RISHIKA\extra\python(UMich)> icacls words.txt /remove "Everyone"
processed file: words.txt
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\rishi\Documents\RISHIKA\extra\python(UMich)> icacls words.txt
words.txt LAPTOP-AN0O1V55\rishi:(R,W)
          NT AUTHORITY\SYSTEM:(I)(F)
          BUILTIN\Administrators:(I)(F)
          LAPTOP-AN0O1V55\rishi:(I)(F)
```

Terminating a specific process using Windows PowerShell

```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> get-process -name "calculator"

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    603      32    23656      42916       1.63   3872   1 Calculator


PS C:\WINDOWS\system32> taskkill /F /PID 3872
SUCCESS: The process with PID 3872 has been terminated.
PS C:\WINDOWS\system32> get-process -name "calculator"
get-process : Cannot find a process with the name "calculator". Verify the process name and call the cmdlet again.
At line:1 char:1
+ get-process -name "calculator"
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (calculator:String) [Get-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand

PS C:\WINDOWS\system32>
```

Terminating multiple processes using Windows PowerShell

```
Administrator: Windows PowerShell

PS C:\WINDOWS\system32> get-process -name "notepad","calculator"

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    590      31    23840      45576       1.48  10760   1 Calculator
    232      12     2520      14028       0.19   6384   1 notepad


PS C:\WINDOWS\system32> taskkill /F /PID 10760
SUCCESS: The process with PID 10760 has been terminated.
PS C:\WINDOWS\system32> taskkill /F /PID 6384
SUCCESS: The process with PID 6384 has been terminated.
PS C:\WINDOWS\system32> get-process -name "notepad","calculator"
get-process : Cannot find a process with the name "notepad". Verify the process name and call the cmdlet again.
At line:1 char:1
+ get-process -name "notepad","calculator"
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (notepad:String) [Get-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand

get-process : Cannot find a process with the name "calculator". Verify the process name and call the cmdlet again.
At line:1 char:1
+ get-process -name "notepad","calculator"
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (calculator:String) [Get-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand

PS C:\WINDOWS\system32>
```