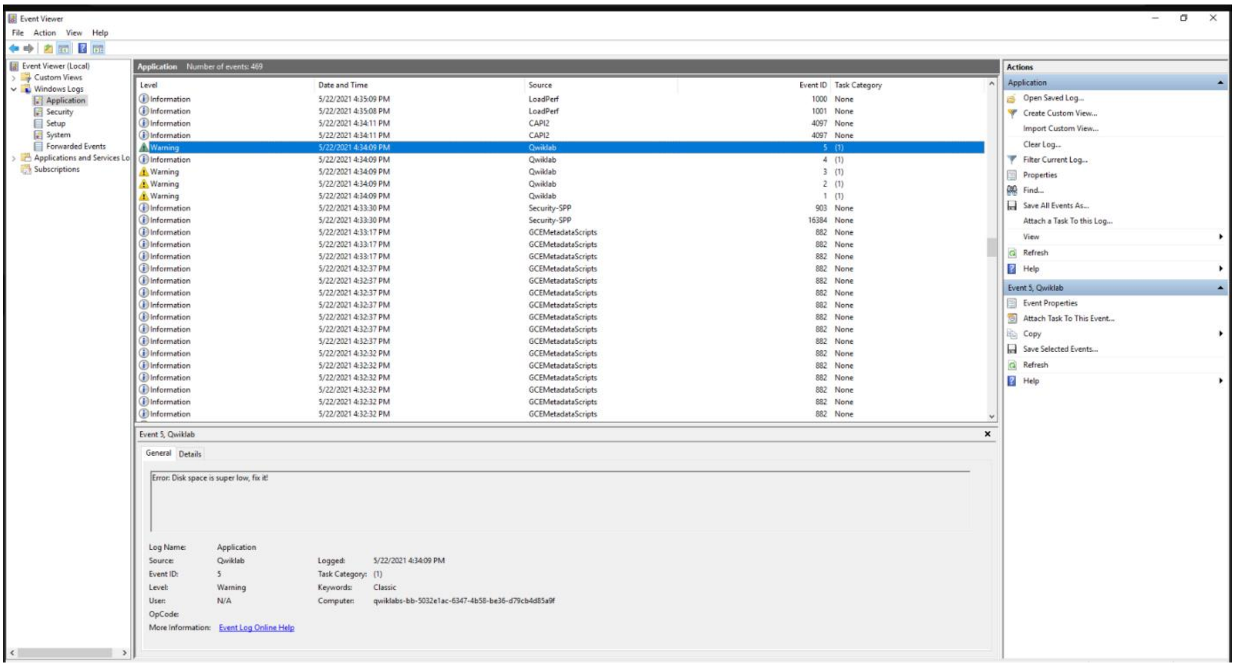
Using Logs to help you track down an issue in Windows

Rishita Gupta

Viewing Logs on Windows:

- Here, application logs are to be examined. To view application logs, click on Windows Logs and select Application
- Locate the logs to be fixed. Click on a log entry to view more details.



Application Number of events: 469

Level	Date and Time	Source	Event ID	Task Category
Information	5/22/2021 4:35:09 PM	LoadPerf	1000	None
Information	5/22/2021 4:35:08 PM	LoadPerf	1001	None
Information	5/22/2021 4:34:11 PM	CAPI2	4097	None
Information	5/22/2021 4:34:11 PM	CAPI2	4097	None
Warning	5/22/2021 4:34:09 PM	Qwiklab	5	(1)
Information	5/22/2021 4:34:09 PM	Qwiklab	4	(1)
Warning	5/22/2021 4:34:09 PM	Qwiklab	3	(1)
Warning	5/22/2021 4:34:09 PM	Qwiklab	2	(1)
Warning	5/22/2021 4:34:09 PM	Qwiklab	1	(1)
Information	5/22/2021 4:33:30 PM	Security-SPP	903	None
Information	5/22/2021 4:33:30 PM	Security-SPP	16384	None
Information	5/22/2021 4:33:17 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:33:17 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:33:17 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:37 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:37 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:37 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:37 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:37 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:37 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:37 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:32 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:32 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:32 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:32 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:32 PM	GCEMetadataScripts	882	None
Information	5/22/2021 4:32:32 PM	GCEMetadataScripts	882	None

Event 5, Qwiklab

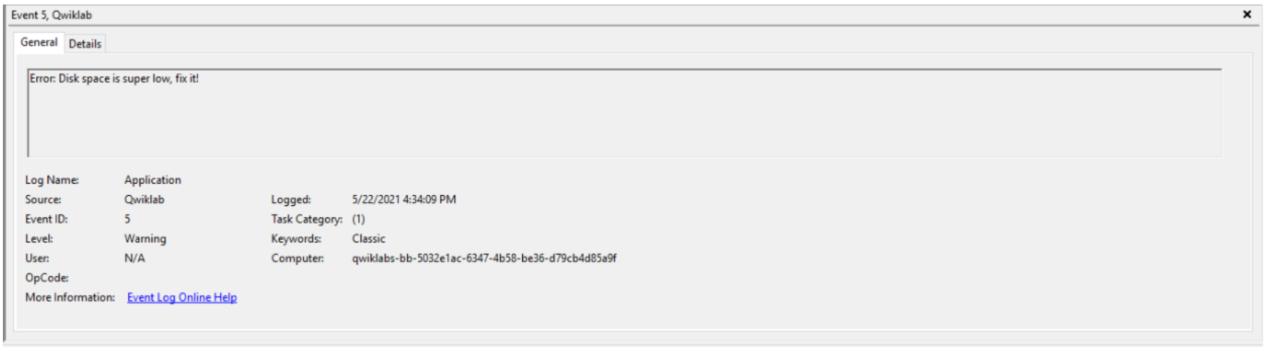
General Details

Error: Disk space is super low, fix it!

Log Name:	Application		
Source:	Qwiklab	Logged:	5/22/2021 4:34:09 PM
Event ID:	5	Task Category:	(1)
Level:	Warning	Keywords:	Classic
User:	N/A	Computer:	qwiklabs-bb-5032e1ac-6347-4b58-be36-d79cb4d85a9f
OpCode:			
More Information:	Event Log Online Help		

1.Low Disk Space:

This log warns about a large file that is taking up disk space, but it does not specify the file name.

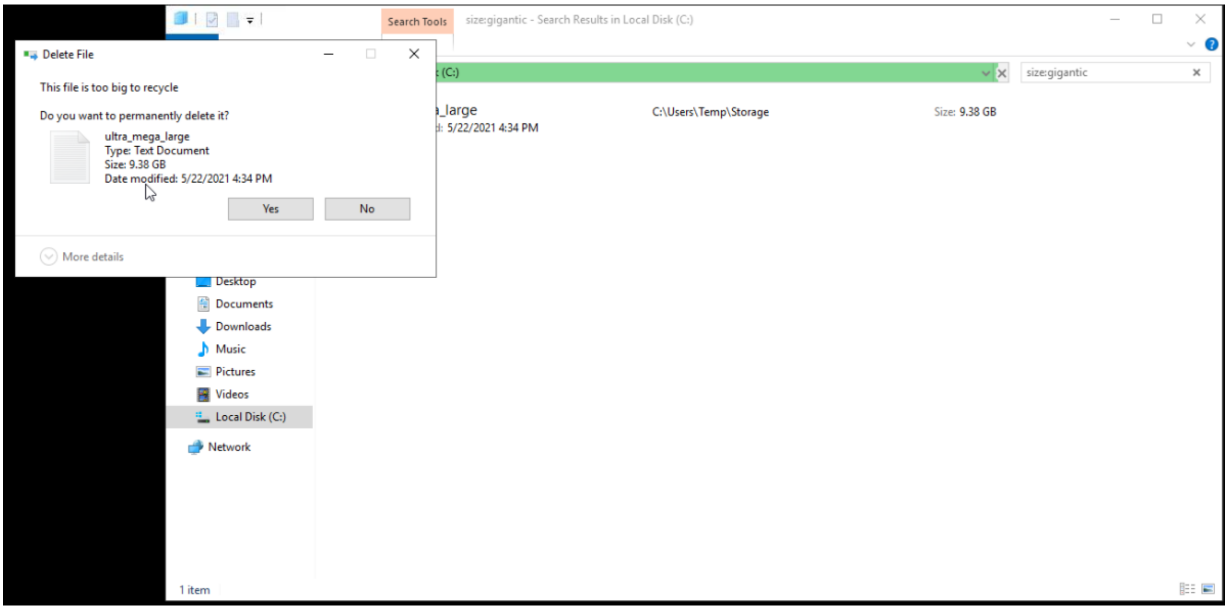


Event 5, Qwiklab

General Details

Error: Disk space is super low, fix it!

Log Name:	Application		
Source:	Qwiklab	Logged:	5/22/2021 4:34:09 PM
Event ID:	5	Task Category:	(1)
Level:	Warning	Keywords:	Classic
User:	N/A	Computer:	qwiklabs-bb-5032e1ac-6347-4b58-be36-d79cb4d85a9f
OpCode:			
More Information:	Event Log Online Help		



Delete File

This file is too big to recycle

Do you want to permanently delete it?

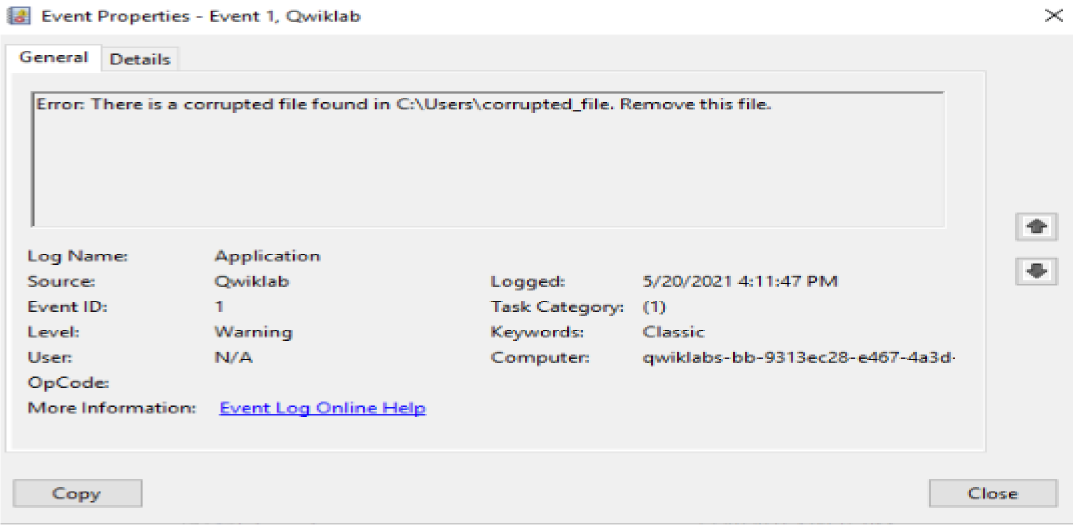
ultra_mega_large
Type: Text Document
Size: 9.38 GB
Date modified: 5/22/2021 4:34 PM

_large
: 5/22/2021 4:34 PM
C:\Users\Temp\Storage
Size: 9.38 GB

Open file explorer and configure the search such that the size of the file is **‘gigantic’** (this locates files whose size exceeds 128 MB). Delete the ‘ultra_merge_large’ file.

2.Corrupted File:

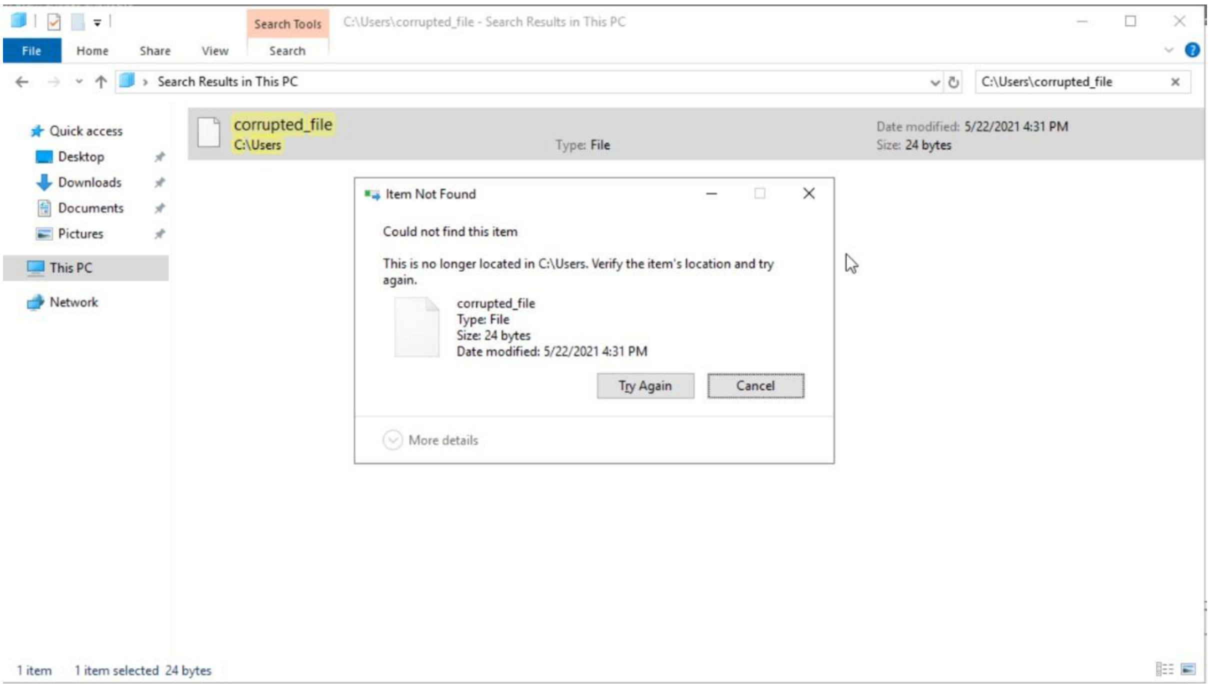
This log warns to remove a corrupted file in the C:\ directory.


Event Properties - Event 1, Qwiklab

Error: There is a corrupted file found in C:\Users\corrupted_file. Remove this file.

Log Name:	Application		
Source:	Qwiklab	Logged:	5/20/2021 4:11:47 PM
Event ID:	1	Task Category:	(1)
Level:	Warning	Keywords:	Classic
User:	N/A	Computer:	qwiklabs-bb-9313ec28-e467-4a3d-
OpCode:			
More Information:	Event Log Online Help		

Search the file explorer for the path specified in the log (C:\Users\corrupted_file). Delete the ‘corrupted_file’.



corrupted_file
C:\Users
Type: File
Date modified: 5/22/2021 4:31 PM
Size: 24 bytes

Item Not Found

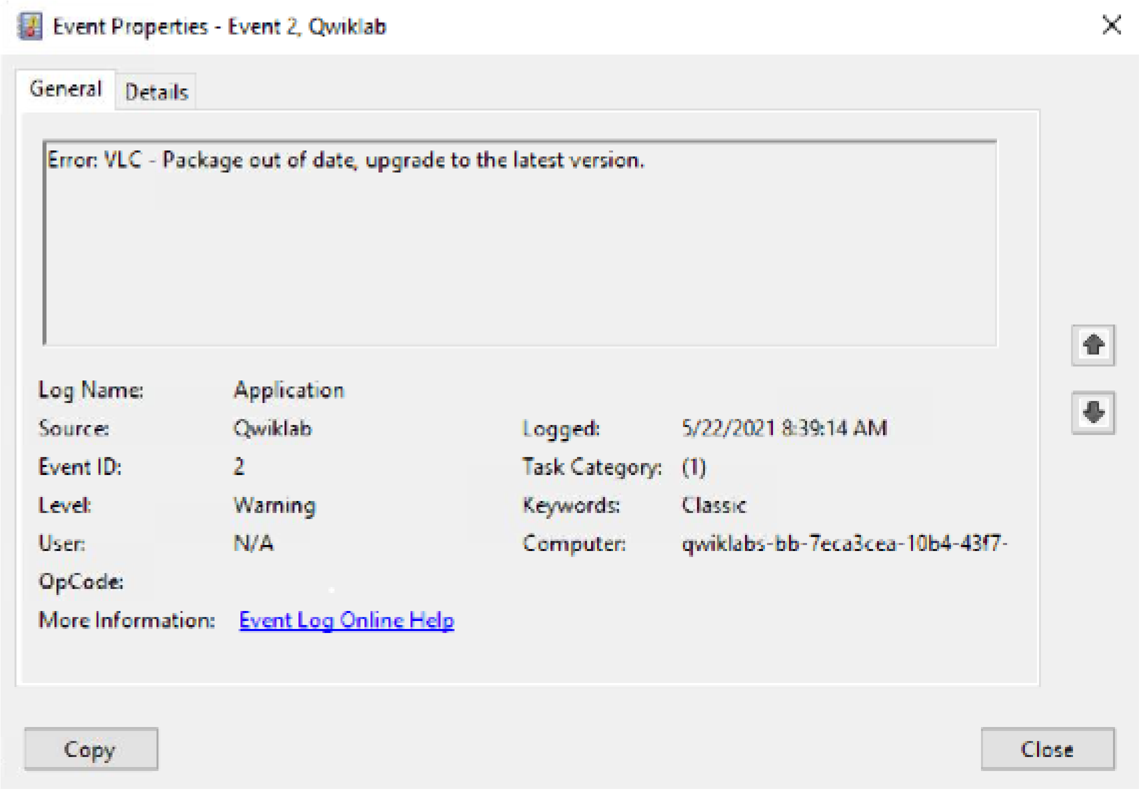
Could not find this item

This is no longer located in C:\Users. Verify the item's location and try again.

corrupted_file
Type: File
Size: 24 bytes
Date modified: 5/22/2021 4:31 PM

3.Update VLC:

This log warns about a software package that is out of date and asks to upgrade to the latest version.



Error: VLC - Package out of date, upgrade to the latest version.

Log Name:	Application		
Source:	Qwiklab	Logged:	5/22/2021 8:39:14 AM
Event ID:	2	Task Category:	(1)
Level:	Warning	Keywords:	Classic
User:	N/A	Computer:	qwiklabs-bb-7eca3cea-10b4-43f7-
OpCode:			
More Information:	Event Log Online Help		

Navigate to the directory where the VLC package is located (C:\Users\qwiklabs\Downloads).

Now the package can be upgraded by executing the following commands:

$VLC_URL = "https://download.videolan.org/vlc/last/win64/";

$DOWNLOAD_DIR = "C:\users\qwiklabs\Downloads\";

$GET_HTML = Invoke-WebRequest $VLC_URL;

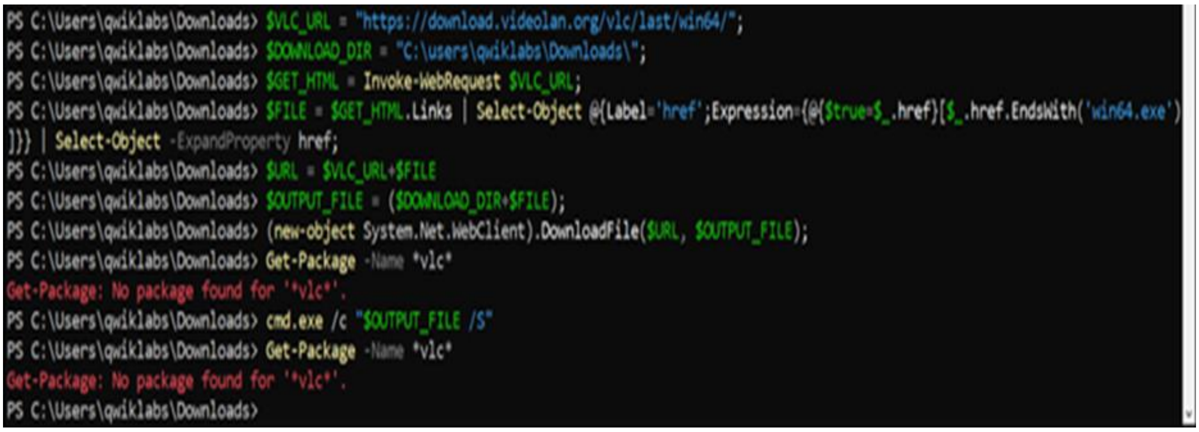
$FILE=$GET_HTML.Links|Select-Object @{Label='href';Expression={@{$true=$_.href}[$_.href.EndsWith('win64.exe')]}} | Select-Object -ExpandPropertyhref;

$URL = ($VLC_URL+$FILE);

$OUTPUT_FILE = ($DOWNLOAD_DIR+$FILE);

(new-object System.Net.WebClient).DownloadFile($URL, $OUTPUT_FILE);

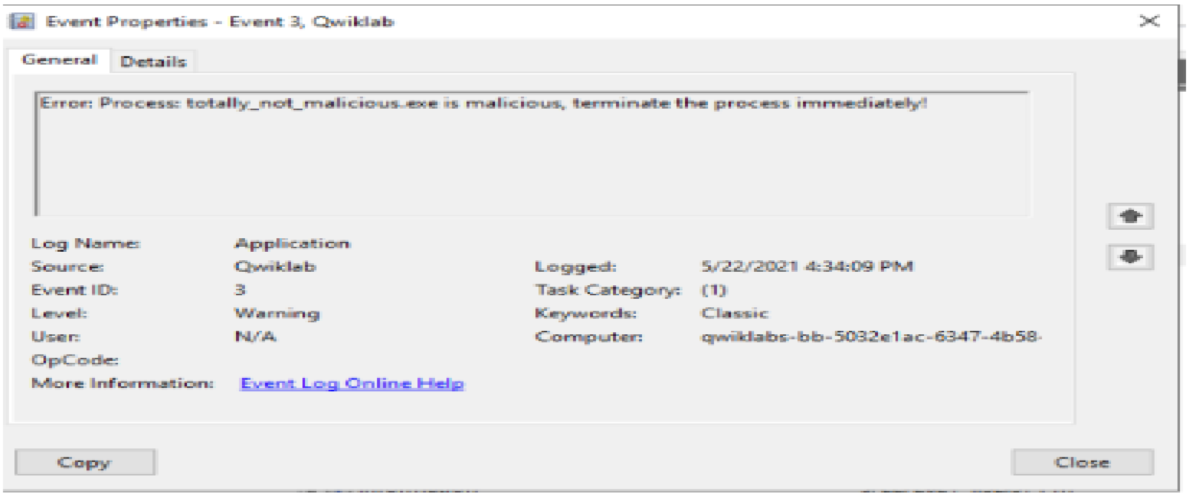
cmd.exe /c "$OUTPUT_FILE /S"



```
PS C:\Users\qwiklabs\Downloads> $VLC_URL = "https://download.videolan.org/vlc/last/win64/";
PS C:\Users\qwiklabs\Downloads> $DOWNLOAD_DIR = "C:\users\qwiklabs\Downloads\";
PS C:\Users\qwiklabs\Downloads> $GET_HTML = Invoke-WebRequest $VLC_URL;
PS C:\Users\qwiklabs\Downloads> $FILE = $GET_HTML.Links | Select-Object @{Label='href';Expression={@{$true=$_.href}[$_.href.EndsWith('win64.exe')
]}} | Select-Object -ExpandProperty href;
PS C:\Users\qwiklabs\Downloads> $URL = $VLC_URL+$FILE
PS C:\Users\qwiklabs\Downloads> $OUTPUT_FILE = ($DOWNLOAD_DIR+$FILE);
PS C:\Users\qwiklabs\Downloads> (new-object System.Net.WebClient).DownloadFile($URL, $OUTPUT_FILE);
PS C:\Users\qwiklabs\Downloads> Get-Package -Name *vlc*
Get-Package: No package found for '*vlc*'.
PS C:\Users\qwiklabs\Downloads> cmd.exe /c "$OUTPUT_FILE /S"
PS C:\Users\qwiklabs\Downloads> Get-Package -Name *vlc*
Get-Package: No package found for '*vlc*'.
PS C:\Users\qwiklabs\Downloads>
```

4.End Malicious Process:

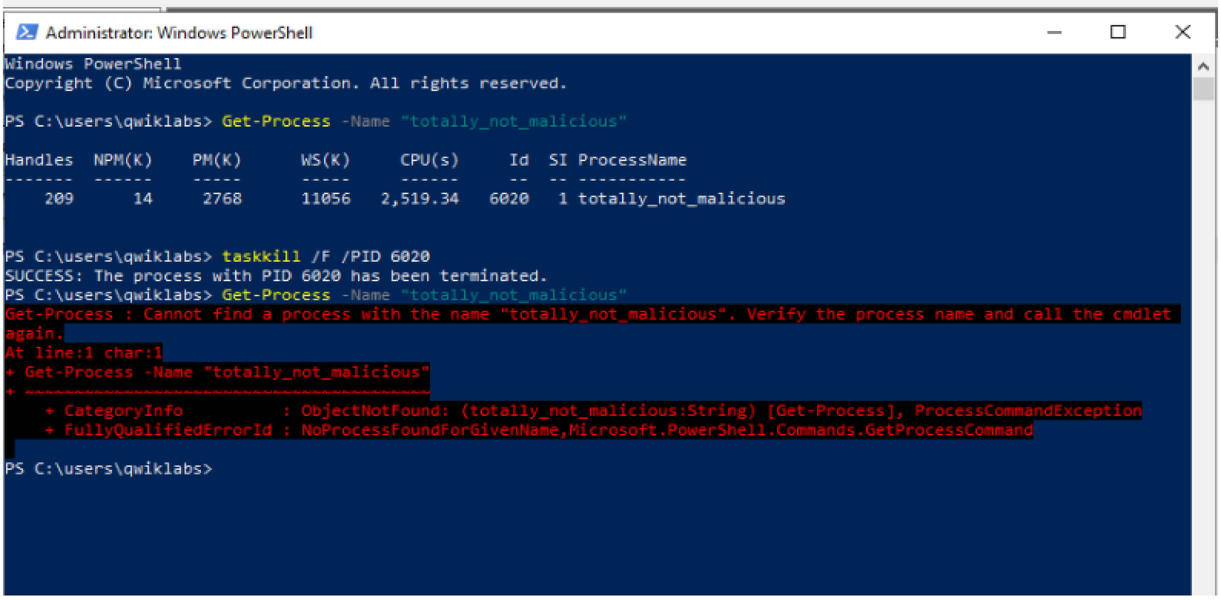
This log warns about a malicious process and asks to terminate it.



Error: Process: totally_not_malicious.exe is malicious, terminate the process immediately!

Log Name: Application
Source: Qwiklab
Logged: 5/22/2021 4:34:09 PM
Event ID: 3
Task Category: (1)
Level: Warning
Keywords: Classic
User: N/A
Computer: qwiklabs-bb-5032e1ac-6347-4b58-
OpCode:
More Information: Event Log Online Help

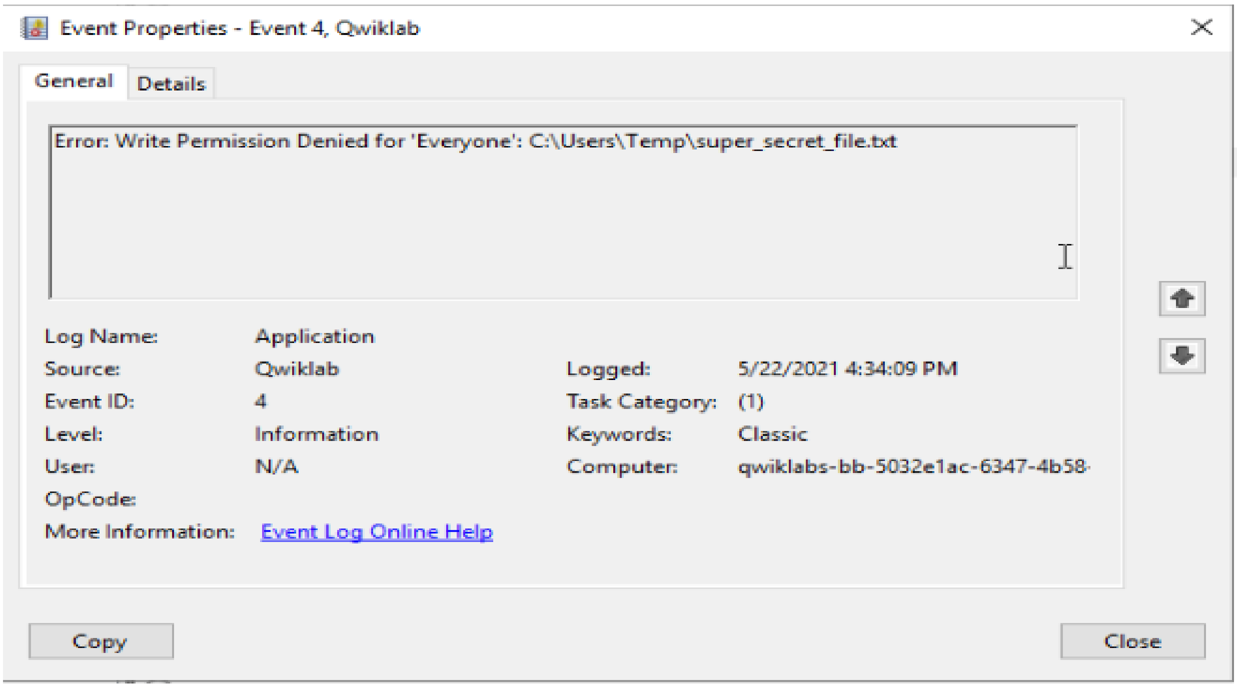
Search for the process by its name (totally not malicious) using **Get-Process -Name [process_name].**This gives the process ID. Terminate the process using **taskkill /F /PID [process_id].** Verify termination using **Get-Process -Name [process_name].**



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

PS C:\users\qwiklabs> Get-Process -Name "totally_not_malicious"

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    209      14     2768      11056   2,519.34   6020   1 totally_not_malicious


PS C:\users\qwiklabs> taskkill /F /PID 6020
SUCCESS: The process with PID 6020 has been terminated.
PS C:\users\qwiklabs> Get-Process -Name "totally_not_malicious"
Get-Process : Cannot find a process with the name "totally_not_malicious". Verify the process name and call the cmdlet
again.
At line:1 char:1
+ Get-Process -Name "totally_not_malicious"
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (totally_not_malicious:String) [Get-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand

PS C:\users\qwiklabs>
```

5.Fix Permissions:

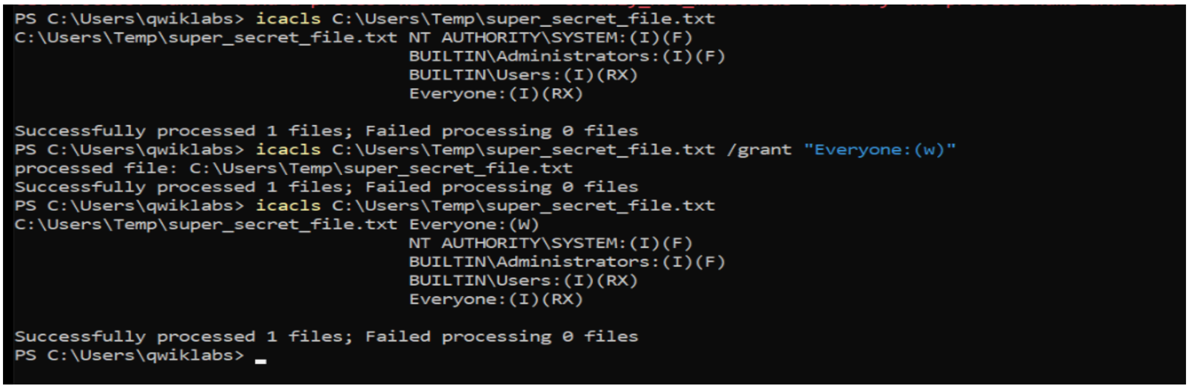
This log warns that write permission is denied for everyone for the file specified in the path.



Error: Write Permission Denied for 'Everyone': C:\Users\Temp\super_secret_file.txt

Log Name: Application
Source: Qwiklab
Logged: 5/22/2021 4:34:09 PM
Event ID: 4
Task Category: (1)
Level: Information
Keywords: Classic
User: N/A
Computer: qwiklabs-bb-5032e1ac-6347-4b58-
OpCode:
More Information: Event Log Online Help

View the existing permissions for the specified file. Grant write permission for Everyone.



```
PS C:\Users\qwiklabs> icacls C:\Users\Temp\super_secret_file.txt
C:\Users\Temp\super_secret_file.txt NT AUTHORITY\SYSTEM:(I)(F)
                                    BUILTIN\Administrators:(I)(F)
                                    BUILTIN\Users:(I)(RX)
                                    Everyone:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\qwiklabs> icacls C:\Users\Temp\super_secret_file.txt /grant "Everyone:(w)"
processed file: C:\Users\Temp\super_secret_file.txt
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\qwiklabs> icacls C:\Users\Temp\super_secret_file.txt
C:\Users\Temp\super_secret_file.txt Everyone:(W)
                                    NT AUTHORITY\SYSTEM:(I)(F)
                                    BUILTIN\Administrators:(I)(F)
                                    BUILTIN\Users:(I)(RX)
                                    Everyone:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\qwiklabs> _
```