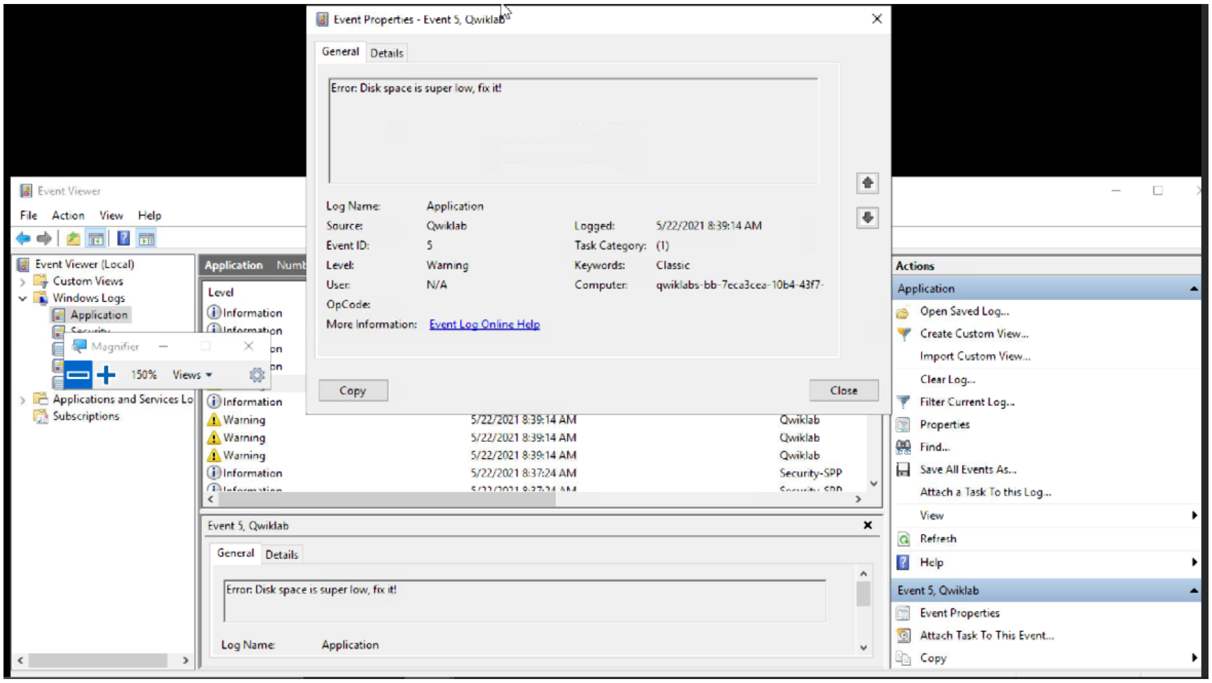
ASSIGNMENT 2
Using logs to track down an issue in windows

Viewing logs on windows:

- To open application logs, go to Windows Logs and click on Application.
- Find the logs that have an issue and to get more details click on any log.



Event Properties - Event 5, Qwiklab

General | Details

Error: Disk space is super low, fix it!

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

```
Information
Warning      5/22/2021 8:39:14 AM   Qwiklab
Warning      5/22/2021 8:39:14 AM   Qwiklab
Warning      5/22/2021 8:39:14 AM   Qwiklab
Information  5/22/2021 8:37:24 AM   Security-SPP
```

Event 5, Qwiklab

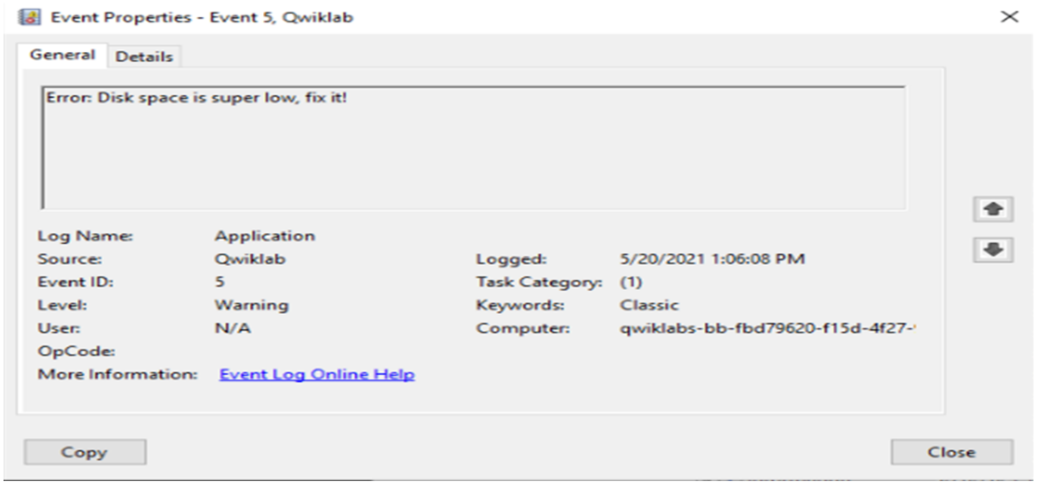
Error: Disk space is super low, fix it!

Log Name: Application

1. **Low Disk Space:**

The log just says that a file is taking up disk space but it doesn't tell the name.

Open File Explorer and search for the file whose space is gigantic and delete that file.



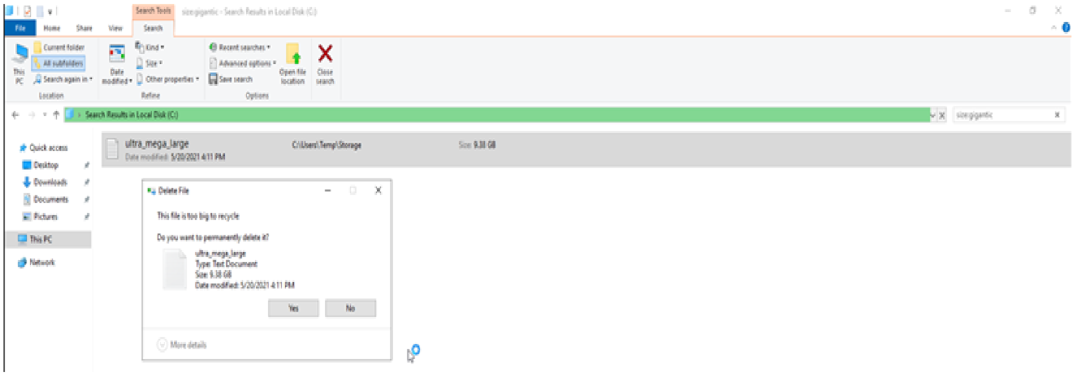
Event Properties - Event 5, Qwiklab

General | Details

Error: Disk space is super low, fix it!

```
Log Name:          Application
Source:            Qwiklab          Logged:          5/20/2021 1:06:08 PM
Event ID:          5                Task Category:   (1)
Level:             Warning          Keywords:        Classic
User:              N/A              Computer:        qwiklabs-bb-fbd79620-f15d-4f27-
OpCode:
More Information:  Event Log Online Help
```

KEERTHANA S
PSG TECH



ultra_mega_large
Date modified: 5/20/2021 4:11 PM
C:\Users\Temp\Storage
Size: 9.38 GB

Delete File

This file is too big to recycle

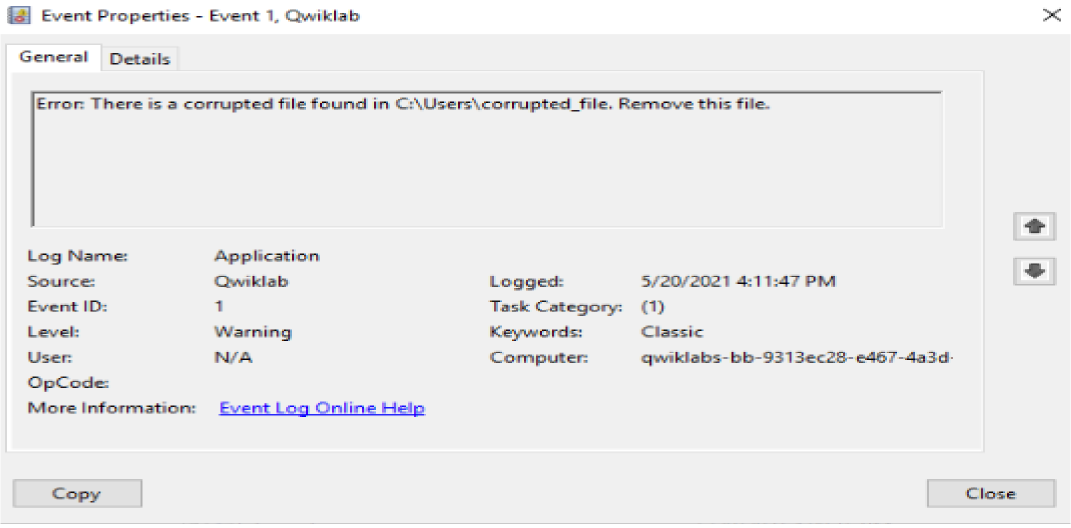
Do you want to permanently delete it?

ultra_mega_large
Type: Text Document
Size: 9.38 GB
Date modified: 5/20/2021 4:11 PM

2. **Corrupted File:**

The log asks to remove a corrupted file in the C:\ Directory.

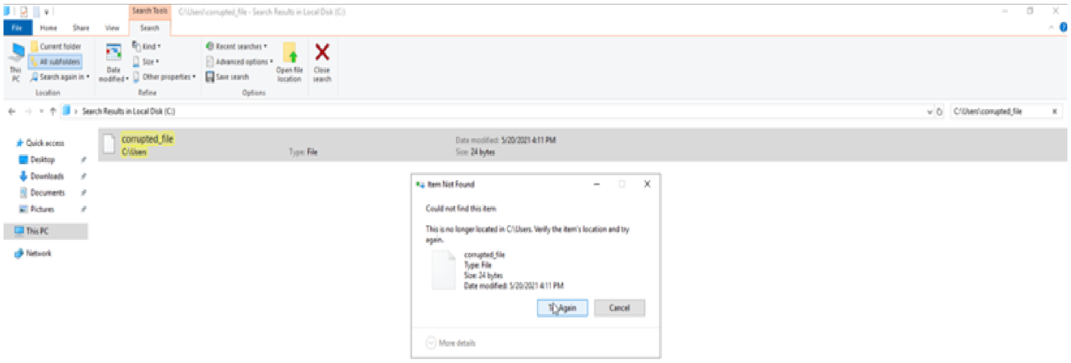
Search for the file using the path - C:\Users\corrupted_file - and delete it.



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		



corrupted_file
C:\Users
Type: File
Date modified: 5/20/2021 4:11 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.

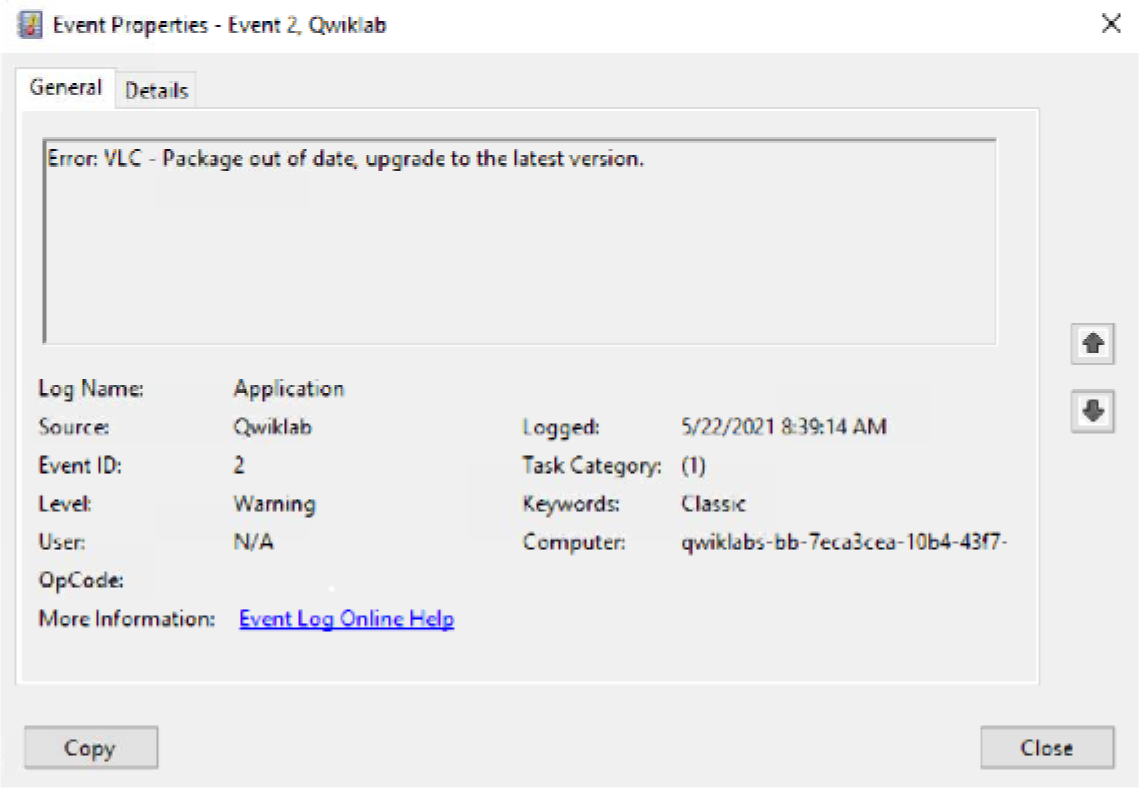
corrupted_file
Type: File
Size: 24 bytes
Date modified: 5/20/2021 4:11 PM

3. Update VLC Player.

This log warns us about an application that is out of date and wants to be updated to the latest version.

Go to the folder where the VLC package (C:\Users\qwiklabs\Downloads) is located and execute 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"
```



Event Properties - Event 2, Qwiklab

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

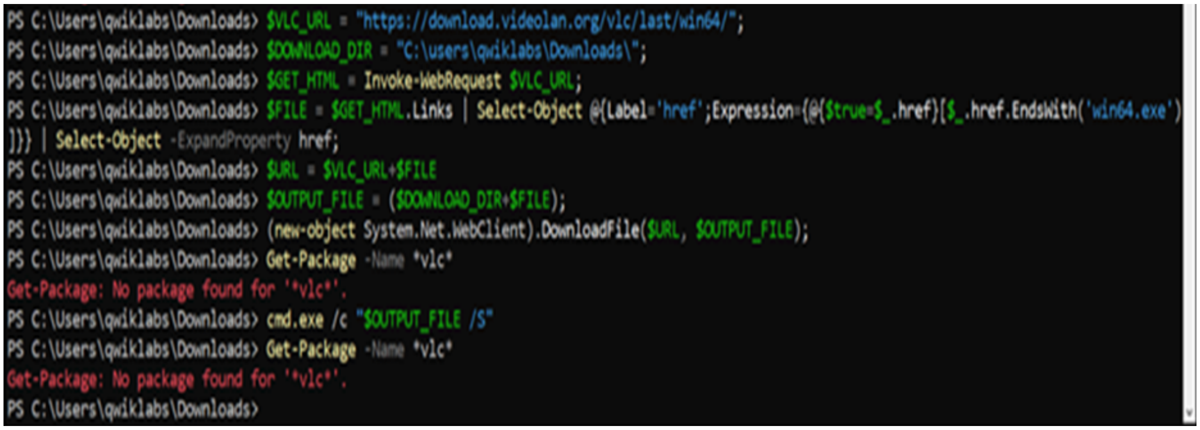
Keywords: Classic

User: N/A

Computer: qwiklabs-bb-7eca3cea-10b4-43f7-

OpCode:

More Information: Event Log Online Help

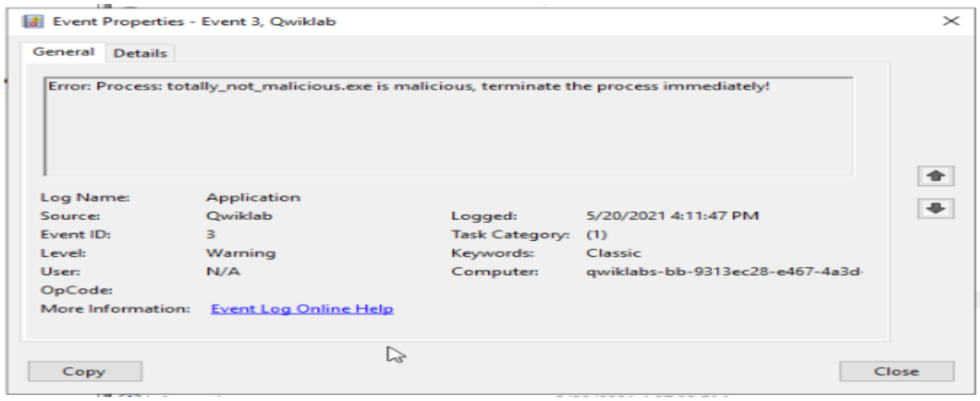


```
PS C:\Users\qwiklabs\Downloads> $VLC_URL = "https://download.videolan.org/vlc/last/win64/";
PS C:\Users\qwiklabs\Downloads> $DOWNLOAD_DIR = "C:\users\qwiklabs\Downloads\";
PS C:\Users\qwiklabs\Downloads> $GET_HTML = Invoke-WebRequest $VLC_URL;
PS C:\Users\qwiklabs\Downloads> $FILE = $GET_HTML.Links | Select-Object @{Label='href';Expression={@{$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

The log warns about a malicious process that needs to be terminated.

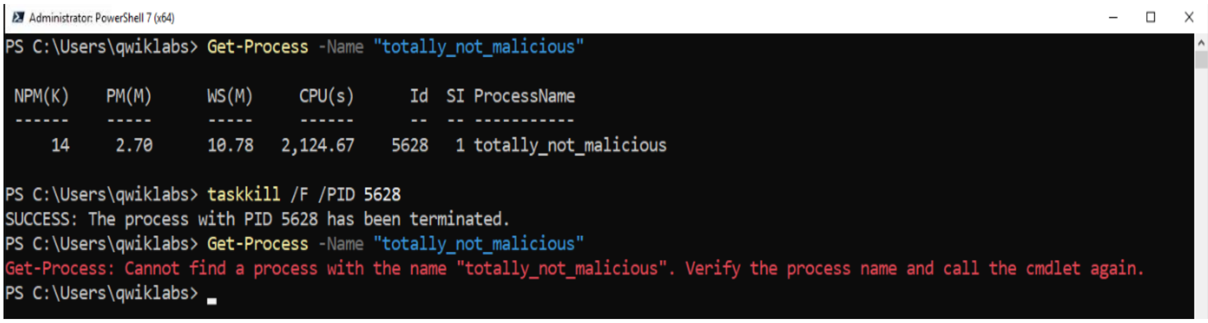
Search for the process by its name using **Get-Process -Name (process name).** Then terminate it with the command **taskkill /pid (process id)**. Verify its existence by using **Get-Process -Name (process name).**



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

Log Name: Application
Source: Qwiklab
Event ID: 3
Level: Warning
User: N/A
OpCode:
More Information: Event Log Online Help

Logged: 5/20/2021 4:11:47 PM
Task Category: (1)
Keywords: Classic
Computer: qwiklabs-bb-9313ec28-e467-4a3d-

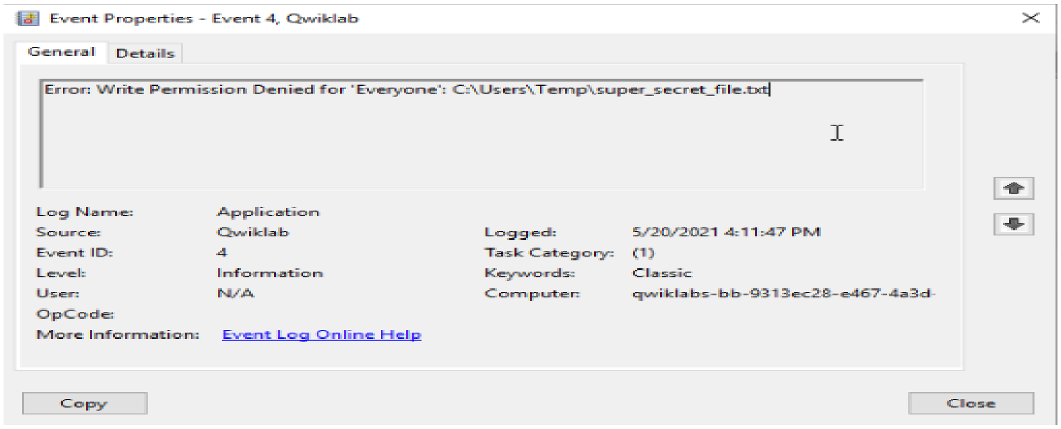


```
PS C:\Users\qwiklabs> Get-Process -Name "totally_not_malicious"

 NPM(K)    PM(M)      WS(M)     CPU(s)      Id  SI ProcessName
 ------    -----      -----     ------      --  -- -----------
     14     2.70      10.78   2,124.67    5628   1 totally_not_malicious

PS C:\Users\qwiklabs> taskkill /F /PID 5628
SUCCESS: The process with PID 5628 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.
PS C:\Users\qwiklabs> _
```

5. Fix permissions

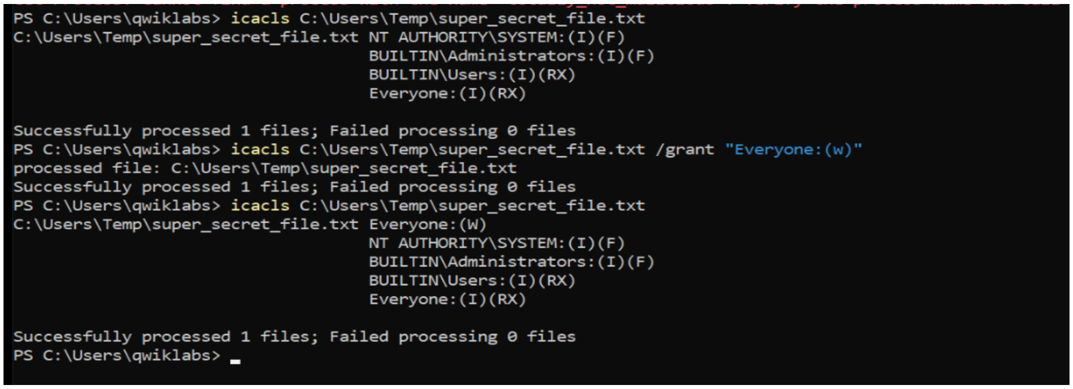
This log specifies that write permission is denied for everyone for a particular file.

View the existing permissions and grant write permission for everyone.



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

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



```
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> _
```