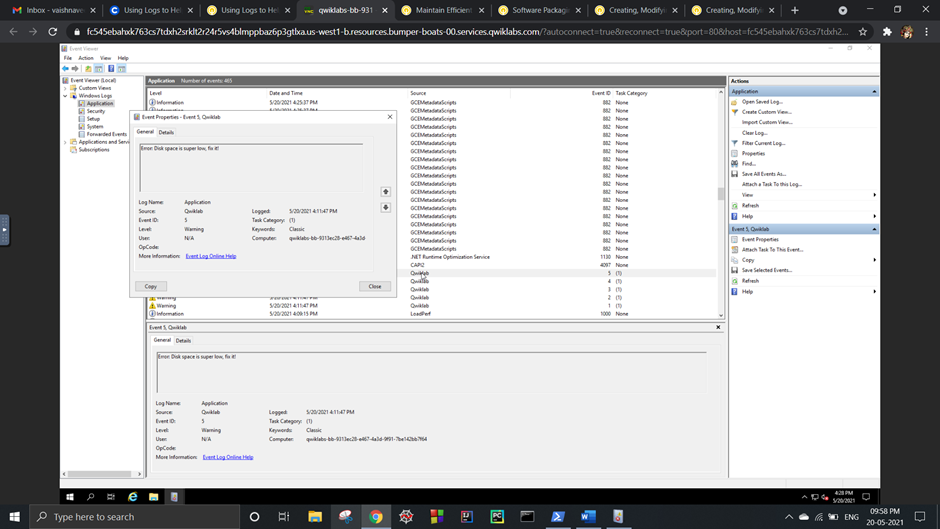
**Using Logs to help you track down an issue in Windows**

**Viewing Logs on Windows:**

**Event Viewer** application is used to view logs in Windows.

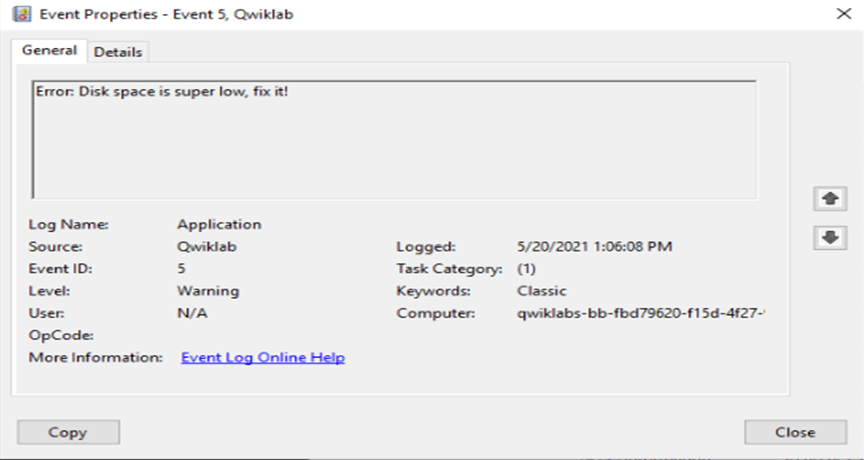
Step 1: Here, application logs are to be examined. To view application logs, click on **Windows Logs** and select **Application**

Step 2: Locate the logs to be fixed. Click on a log entry to view more details.

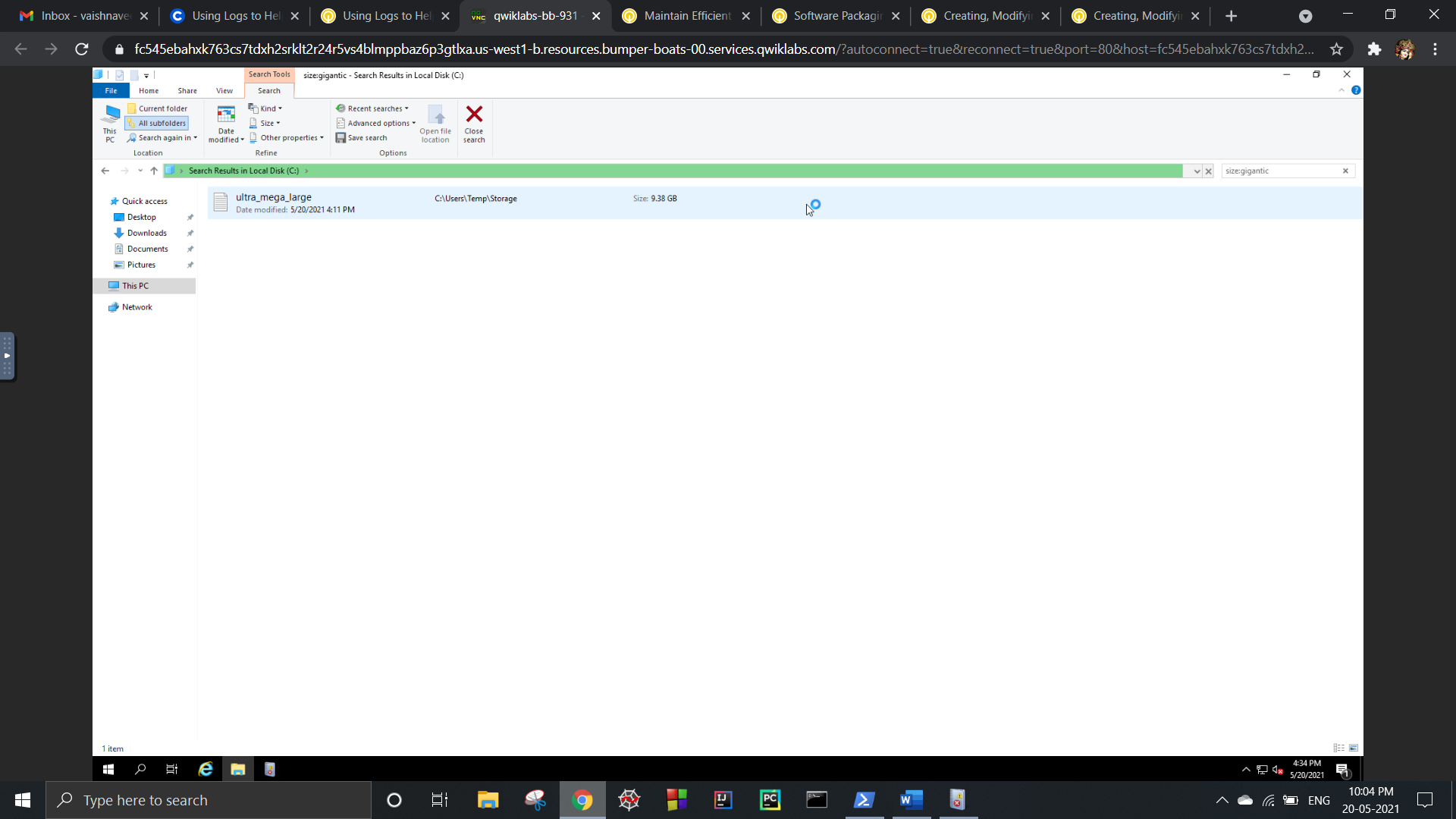


**1.Low Disk Space:**

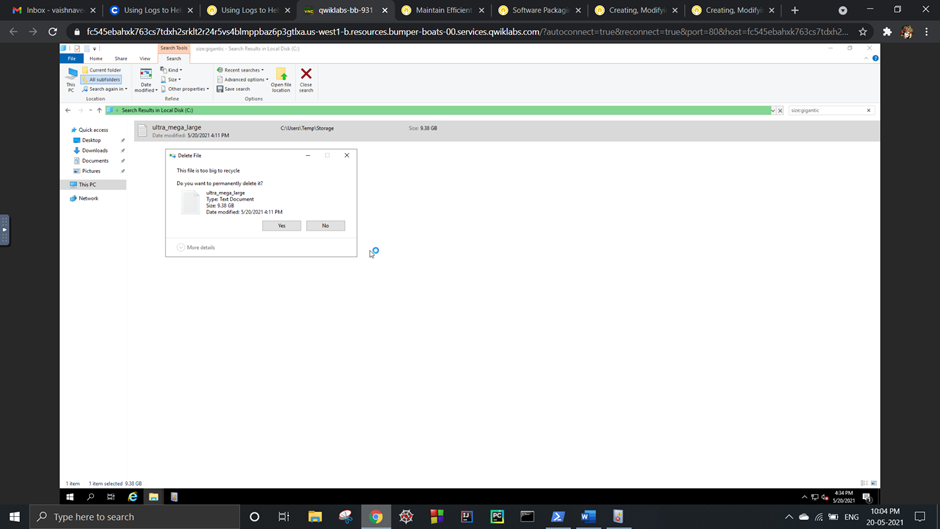
This log warns about a large file that is taking up disk space, but it does not specify the file name.



Step 1: Open file explorer and configure the search such that the size of the file is **‘gigantic’** (this locates files whose size exceeds 128 MB).

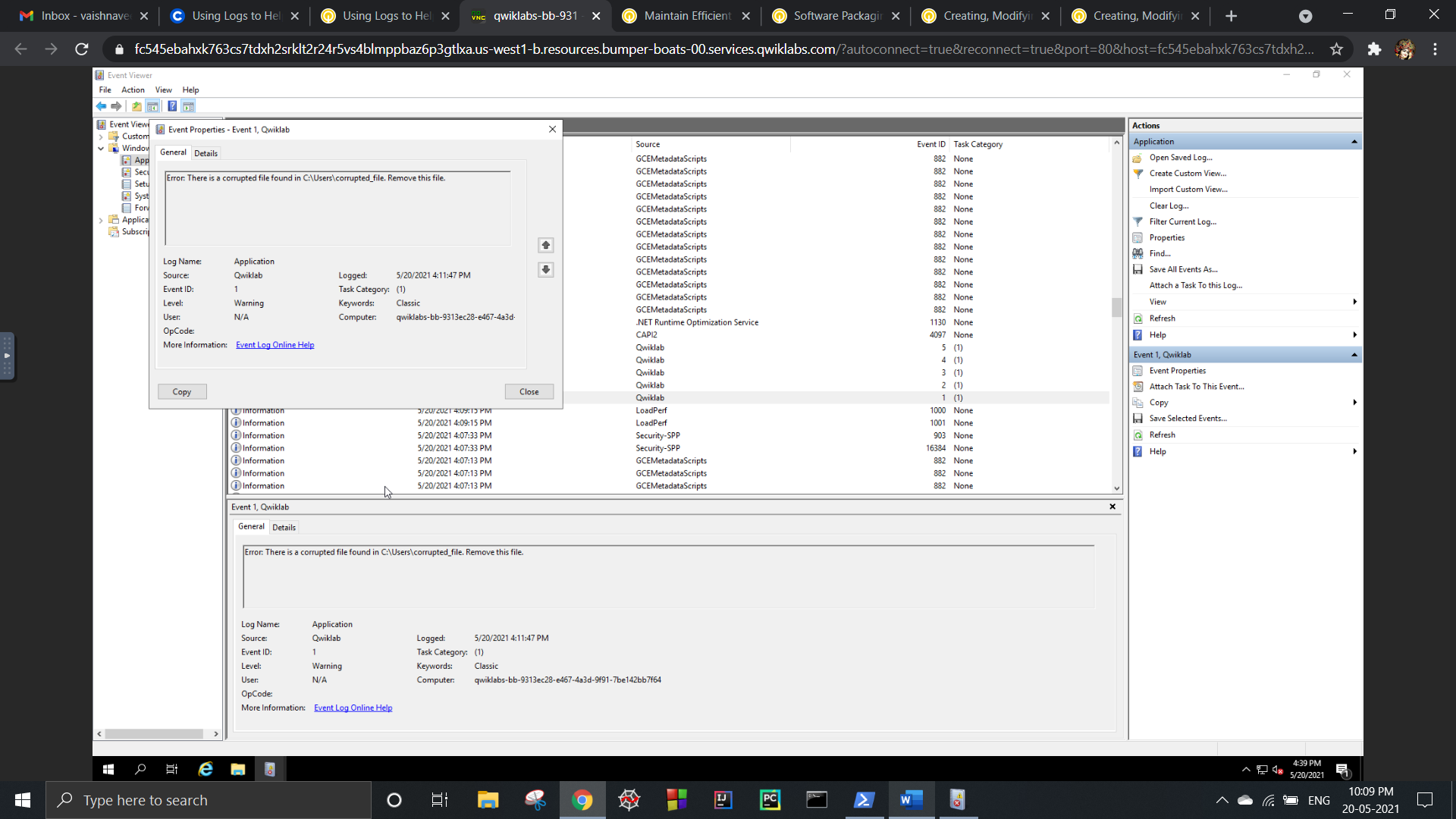


Step 2: Delete the ‘ultra\_merge\_large’ file (size - 9.38 GB).

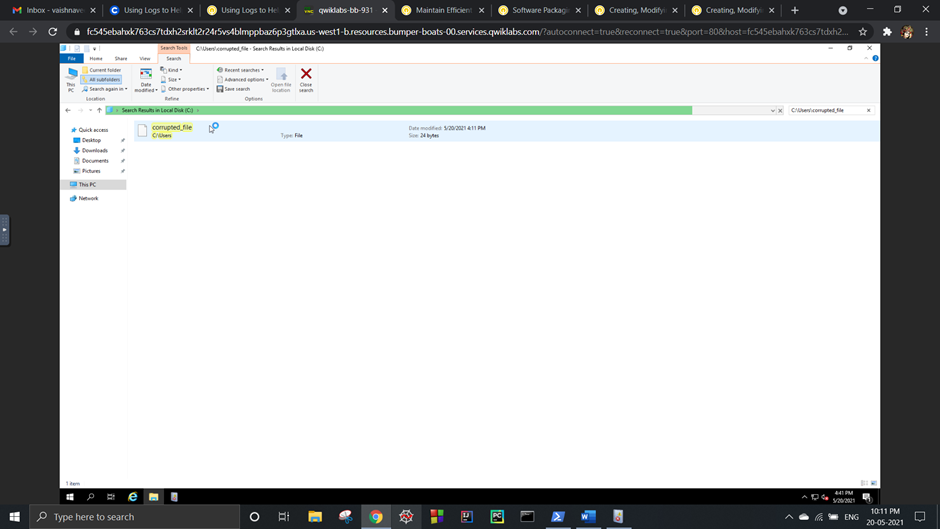


**2.Corrupted File:**

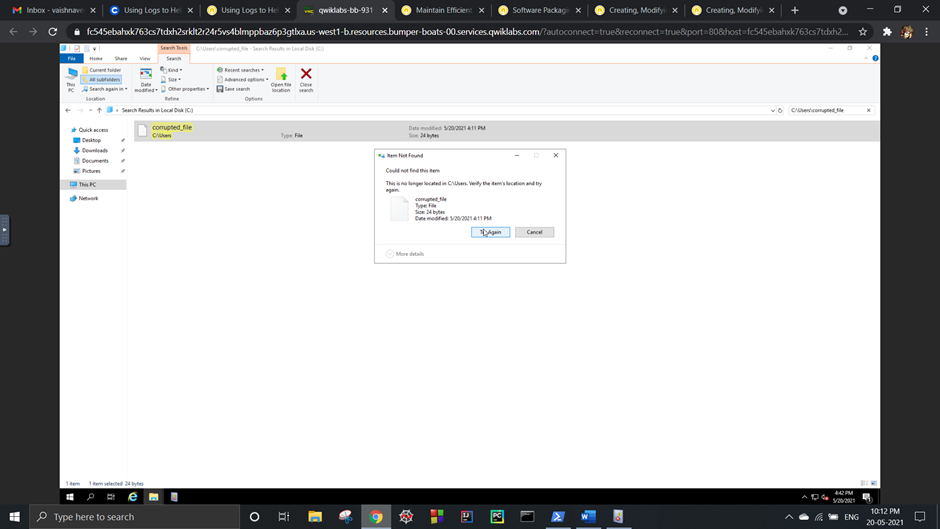
This log warns to remove a corrupted file in the C:\ directory.



Step 1: Search the file explorer for the path specified in the log (C:\Users\corrupted\_file).

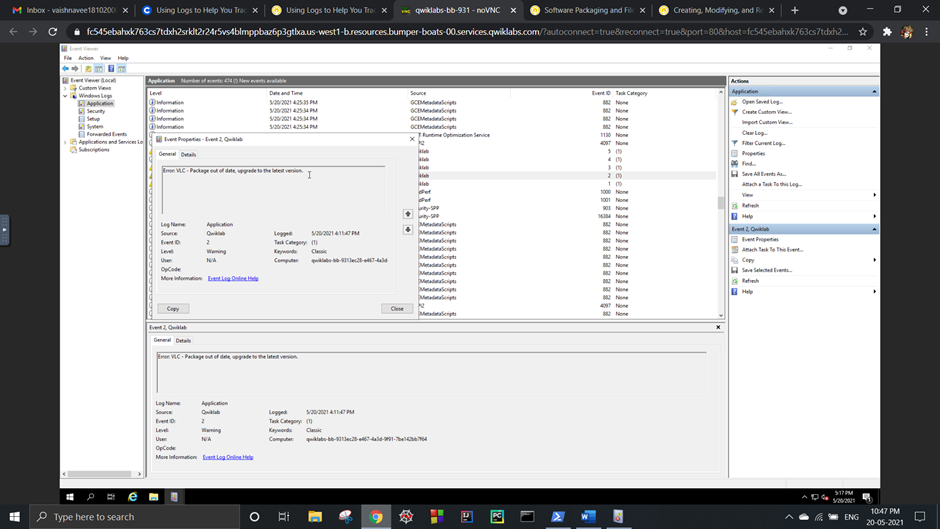


Step 2: Delete the ‘corrupted\_file’.



**3.Update VLC:**

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



Step 1: Navigate to the directory where the VLC package is located (C:\Users\qwiklabs\Downloads).

Step 2: 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 -ExpandProperty href;

$URL = ($VLC\_URL+$FILE);

$OUTPUT\_FILE = ($DOWNLOAD\_DIR+$FILE);

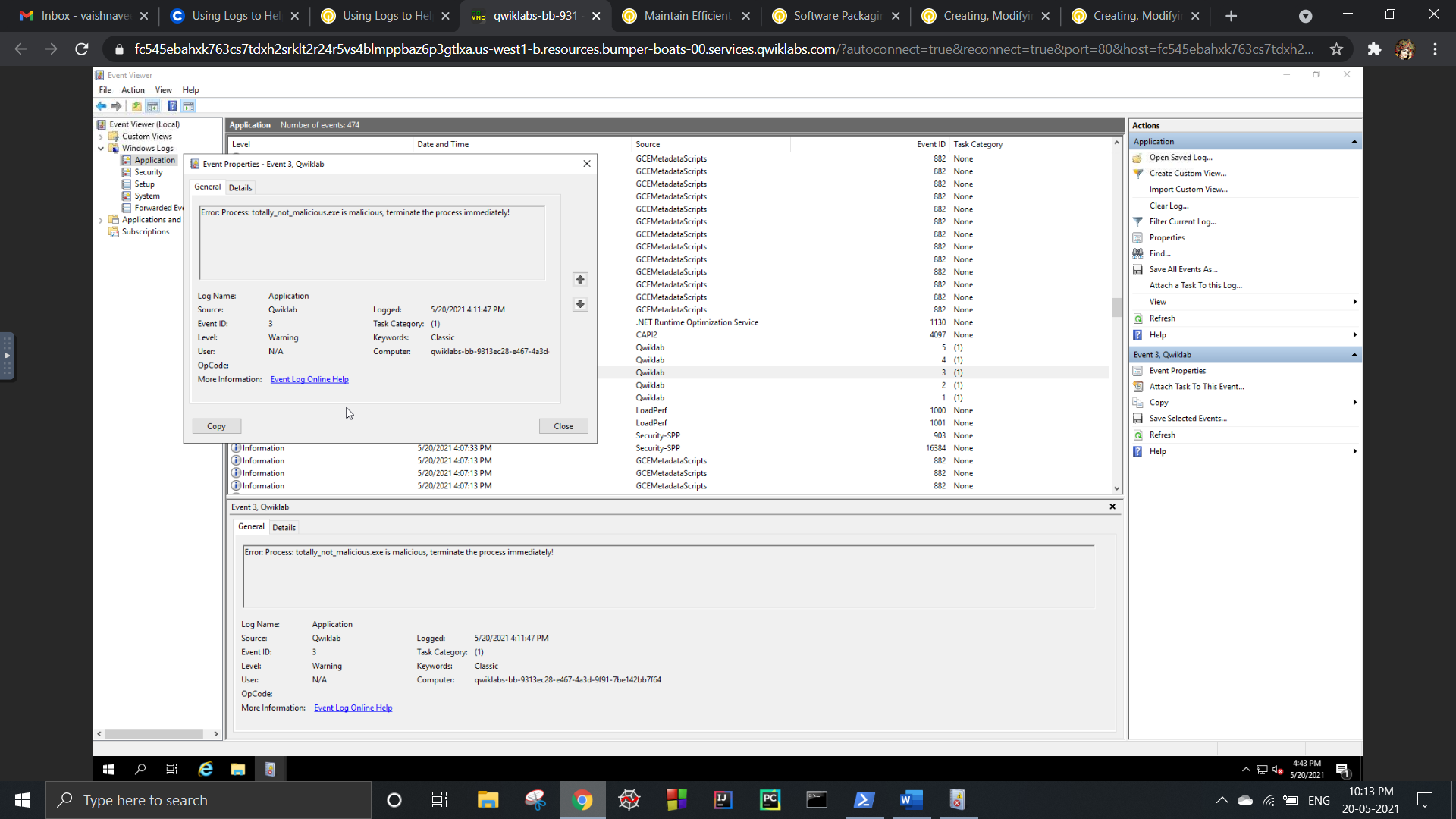
(new-object System.Net.WebClient).DownloadFile($URL, $OUTPUT\_FILE);

cmd.exe /c "$OUTPUT\_FILE /S"



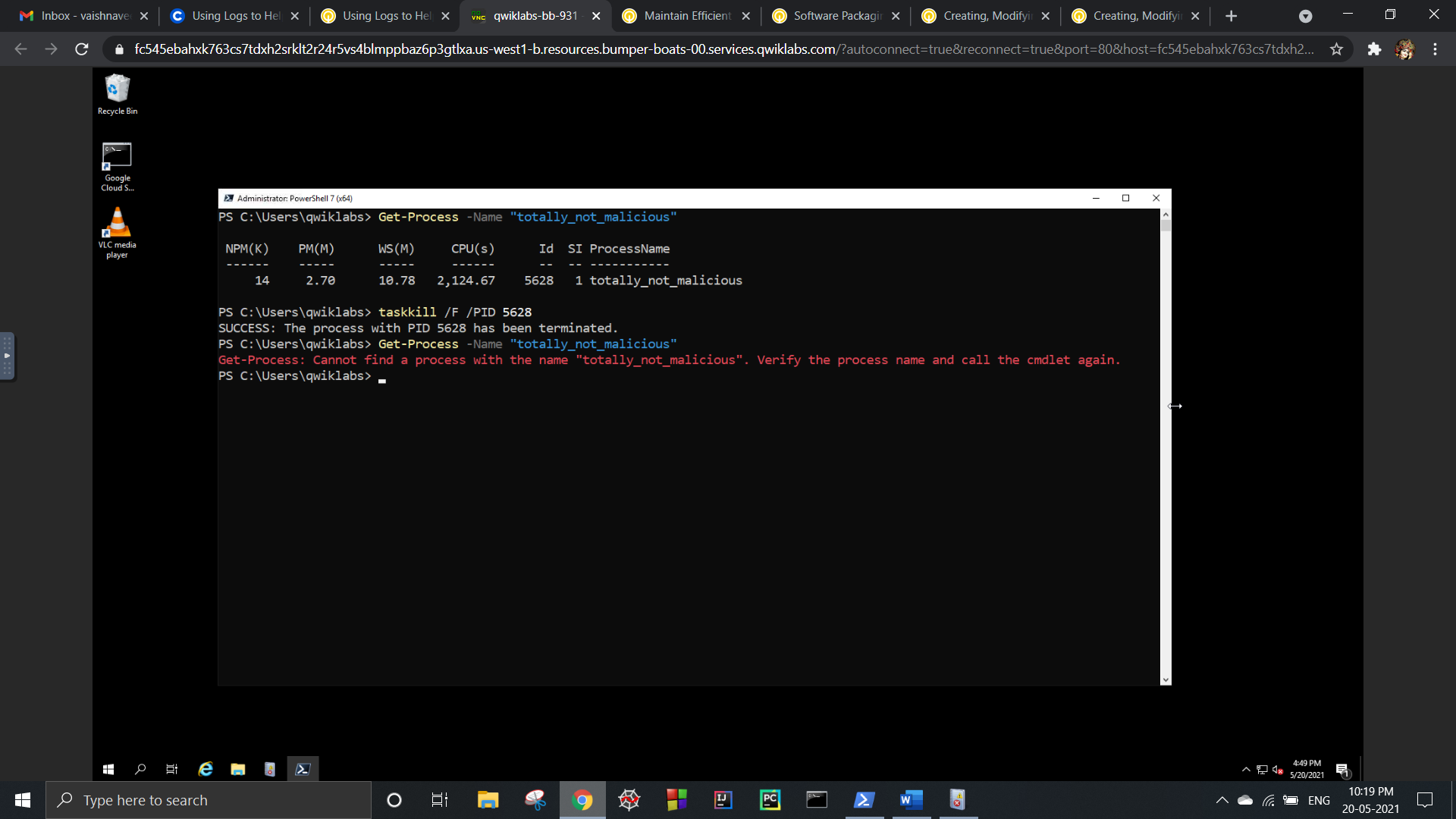
**4.End Malicious Process:**

This log warns about a malicious process (totally\_not\_malicious.exe) and asks to terminate it.



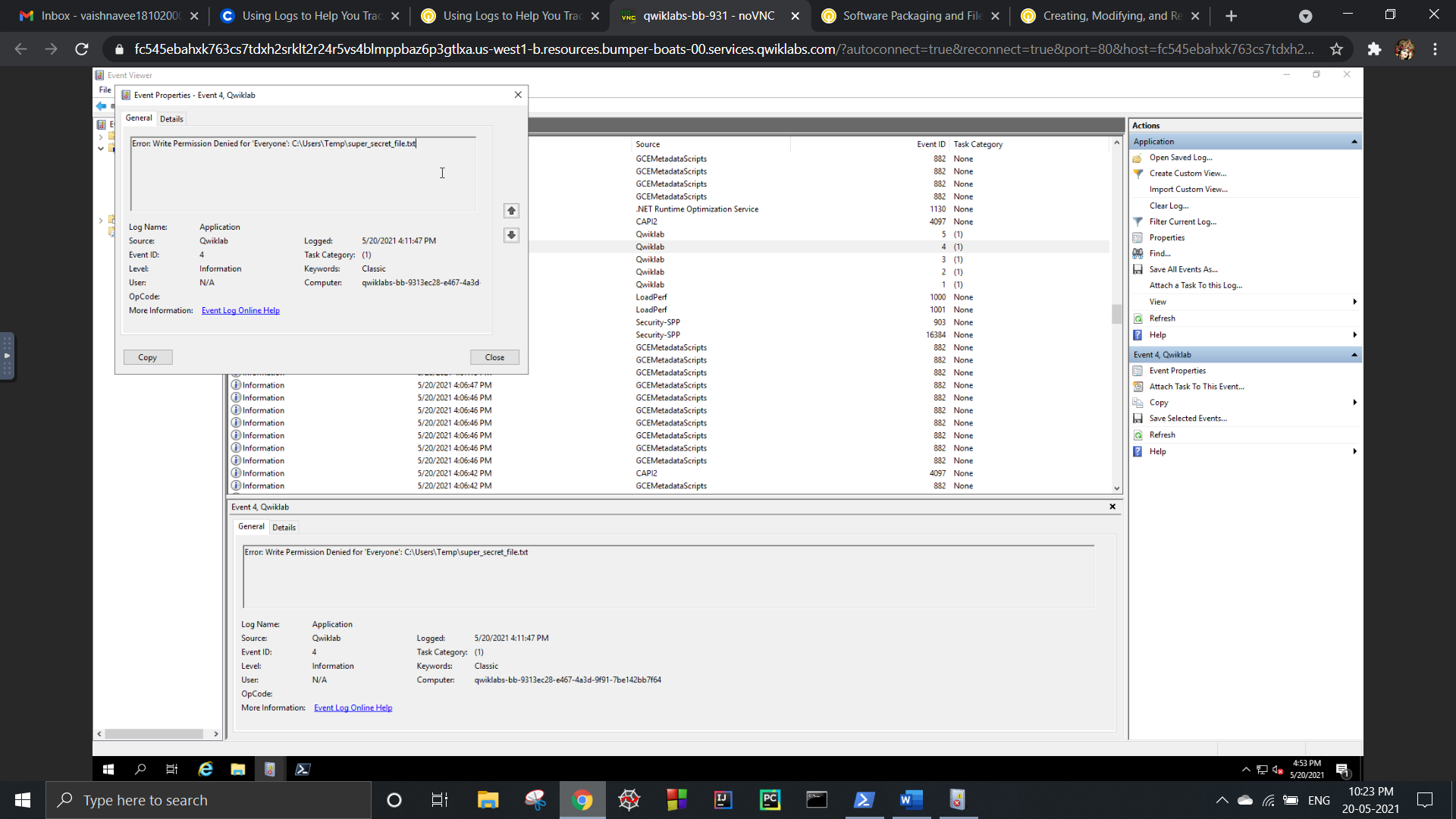
Step 1: Search for the process by its name (totally not malicious) using **Get-Process -Name [process\_name].** This gives the process ID.

Step 2: Terminate the process using **taskkill /F /PID [process\_id].** Verify termination using **Get-Process -Name [process\_name].**



**5.Fix Permissions:**

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



Step 1: View the existing permissions for the specified file using icacls C:\Users\Temp\super\_secret\_file.txt

Step 2: Grant write permission for Everyone using icacls C:\Users\Temp\super\_secret\_file.txt /grant “Everyone:(w)”.

