2022

Windows 10 Forensic Report

TASK 1: Windows Recycle Bin

Experiment: Place a file in the Recycle Bin and then Change its Size

Analyst: Adra Gonazlez

Burlington, Vermont 05401
Champlain College DFIR
The Leahy Center for Digital Investigation

11/03/2022

Table of Contents

I. Artifact name and description

$Recycle.Bin : A hidden folder that contains files that the user has deleted, but has not fully erased from the system. When a file gets placed into the Recycle Bin, two new files get created and are stored in the $Recycle.Bin folder, separated by the user's SID. The first new file starts with $I and is followed by a 6 character random string. This file contains the metadata for the original file, including the filename, date of deletion, path, and size. The second file that is created starts with $R followed by the same random 6 character string. This file will contain the contents of the original file. A pair of $I and $R files indicates that a file is in the Recycle Bin. Just a $I file indicates that the file was restored from the Recycle Bin. Red X's over the $I or $R file icons can indicate that the file was deleted from the Recycle Bin. Nothing in the $Recycle.Bin folder can indicate that nothing was ever placed there, or the files were fully deleted.

II. Tools used for Extraction

FTK Imager:

Author: AccessData
GUI
Brief tool description: FTK Imager is a tool that collects electronic evidence by creating Data Previews, Images, and/or Hash Reports.

RBCmd.exe:

Author: Eric Zimmerman
CLI
Brief tool description: A Recycle Bin Artifact Parser

III. Hashes of Evidence

Artifacts 1:

SHA1: 2635e178305701111d3ec3f6dae27c2b263b6bb2
MD5: 5cd7c1d8b1d988b9a6140c8aa3ecd8e0

Artifacts 2:

SHA1 checksum: bb3a62e083433078e7b12948ca148130a5d89041
MD5 checksum: 3966d01c4204ea24adbeade7e30ee65b

Artifacts 3:

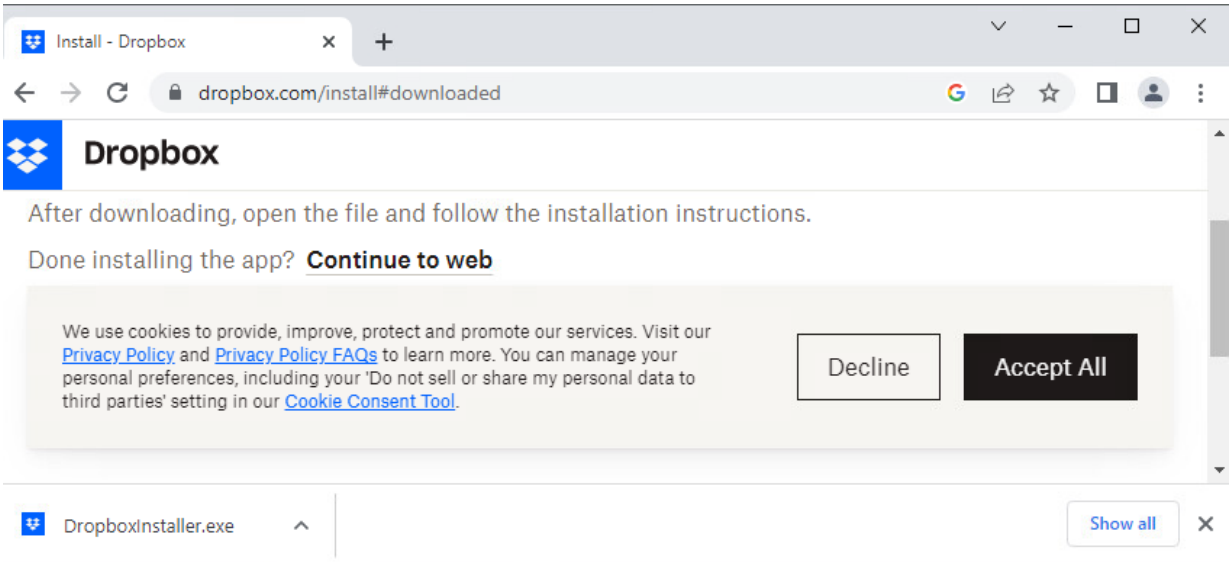
SHA1 checksum: fcc82945bdbb5b7dc24de02d718ca3d4257ae731
MD5 checksum: 4768e4a552b4d1d4f92d3186c4b0bf2b

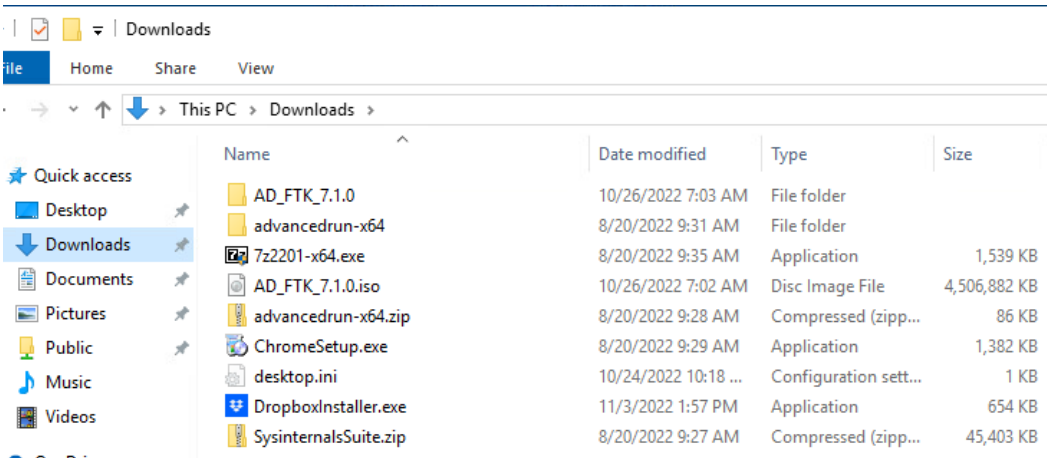
IV. Description of Experiment

Experiment: Place a file in the Recycle Bin and Change its Size

Anticipated steps to complete experiment:

1. **Download the file**
    a. Download DropboxInstaller.exe from dropbox.com/install to C:\Users\IEUser\Downloads





2. **Delete the file**
    a. Open File Explorer, highlight DropboxInstaller.exe, right-click, select "Delete"
3. **Use FTK Imager to locate and recover any files in $Recycle.Bin folder**
    a. Export files located in $Recycle.Bin under IEUser SID to an Artifacts 1 folder located C:\Users\IEUser\Desktop\Artifacts 1

4. **Analyze the recovered files**
    a. Use RBDmd.exe to analyze the files in the Artifacts folder
    b. Open the Command Prompt and type the command: RBCmd.exe -d "Artifacts 1"
5. **Change size of Recycle Bin**
    a. Right click Recycle Bin icon then select “Properties”
    b. Change the size from 4095 MB to 100 MB
6. **Repeat steps 3 - 5**
    a. Step 3: Export the files to a separate Artifacts 2 folder
    b. Replace Artifacts 1 with Artifacts 2
    c. Step 5: Change size of Recycle Bin from 100 MB to 5000 MB
7. **Repeat steps 3 and 4**
    a. Step 3: Export the files to a separate Artifacts 3 folder
    b. Step 4: Replace Artifacts 2 with Artifacts 3
8. **Make an image**
    a. Use FTK imager to make an image of each Artifacts folder
    b. Export images to separate to “Image” folders in C:\Users\IEUser\Desktop\Image
    c. These folder will be titled Image 1 Image 2 and Image 3
9. **Record the results**
    a. Take screenshots of file names, properties, pop ups, and program output.
    b. Take hash of evidence in output folder with FTK Imager

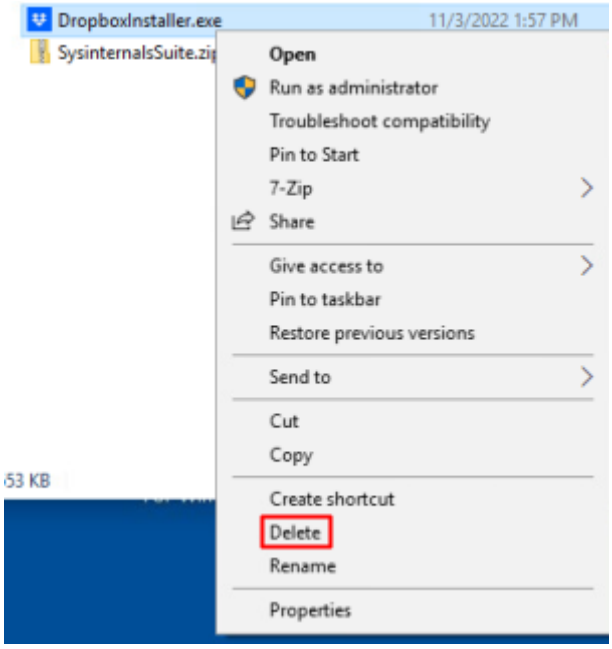
V. Experiment and Analysis

Experiment

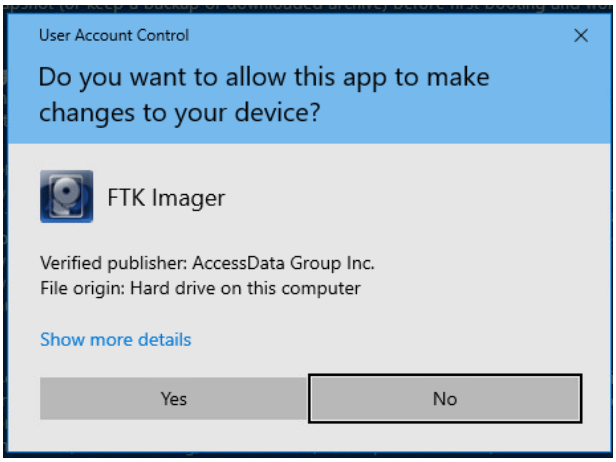
1. **Download the file**

File Name	File Extension	File Size	Where the File was Found	File Path
DropboxInstaller	.exe	653 KB 669,552 bytes	dropbox.com/install	C:\Users\IEUser\Downloads

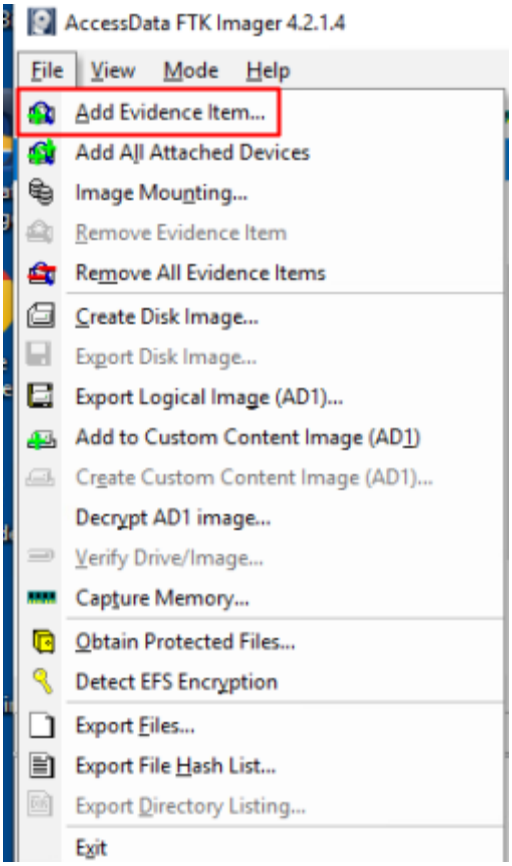
2. **Delete the file**
   First, I opened File Explorer and navigated to C:\Users\IEUser\Downloads. Next, I highlighted DropboxInstaller.exe, right-clicked, and selected “Delete”



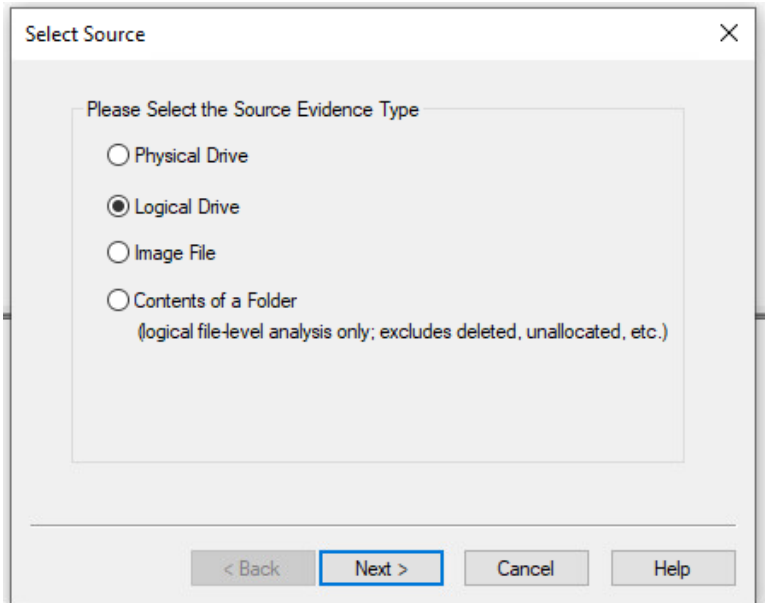
3. **Use FTK Imager to locate and recover any files in $Recycle.Bin folder**
   To recover the files, I opened FTK Imager. The pop up below appeared, and I selected “Yes”.



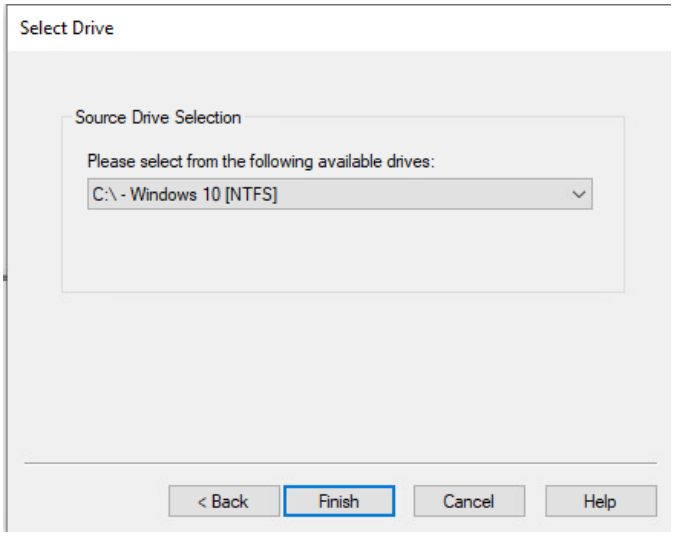
I added the C: drive as an evidence item. To do this you first select File then Add Evidence Item.



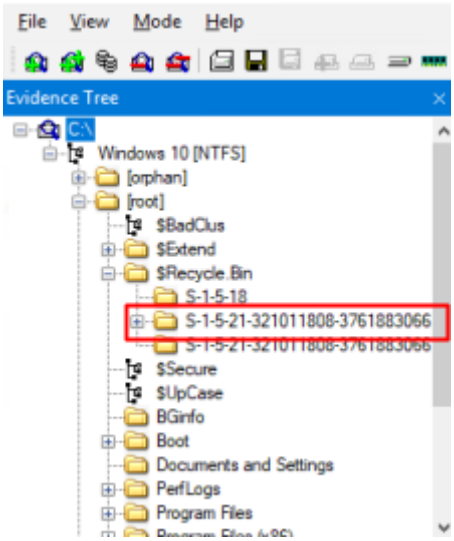
Selected Logical Drive



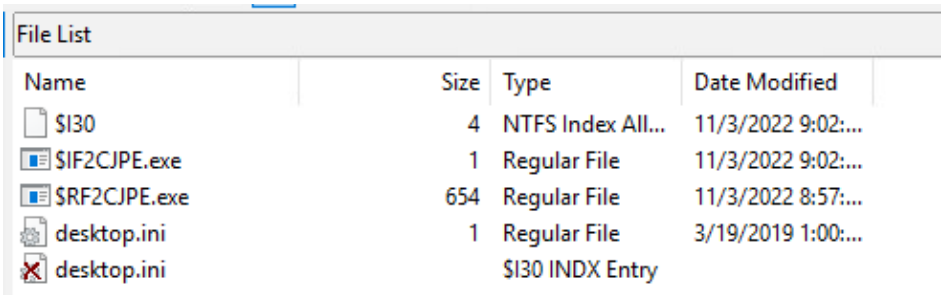
Selected C:\ - Windows 10 [NTFS] and finish



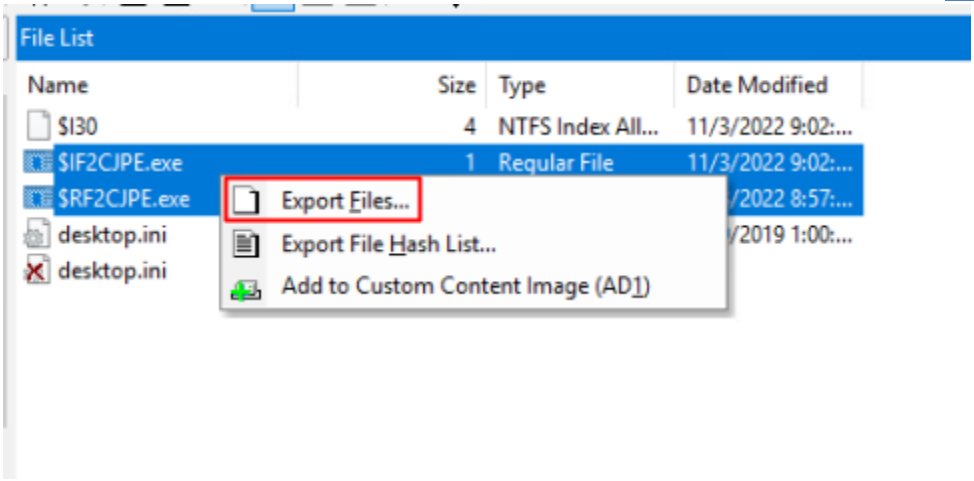
I then navigated to my SID folder (S-1-5-21-32101808-3761883066-353627080-1000) in $Recycle.Bin



After opening the correct SID folder, to the right will be a section called file list. The files I viewed are below:

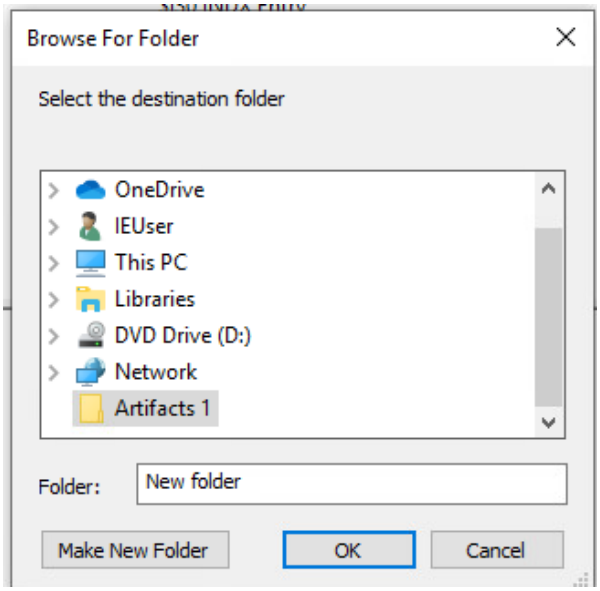


Next I highlighted all of the files, right clicked and selected Export Files…

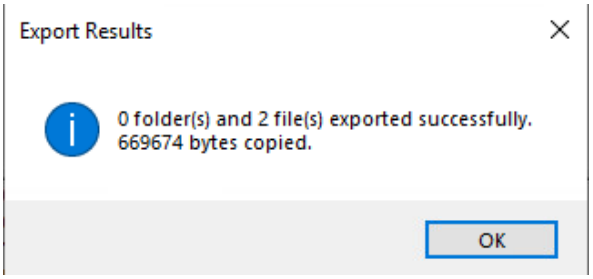


**Note: I went back and exported $I30, desktop.ini and desktop.ini to the same folder

In the export menu I created a folder titled Artifacts 1

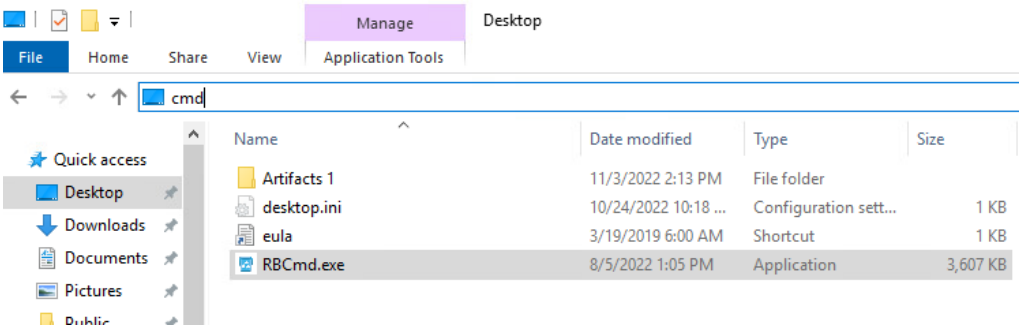


I then exported the files to C:\Users\IEUser\Desktop\Artifacts 1 and received this confirmation.

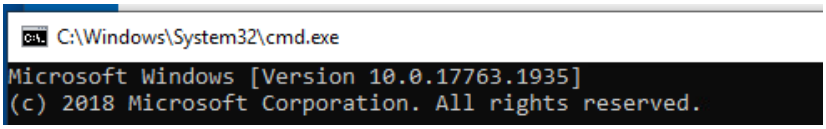


4. **Analyze the recovered files**

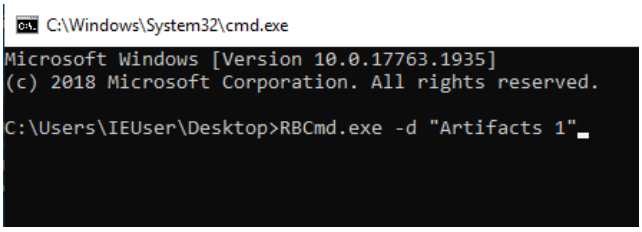
I first typed cmd into the file location bar.



Hitting the enter key brought up this menu:



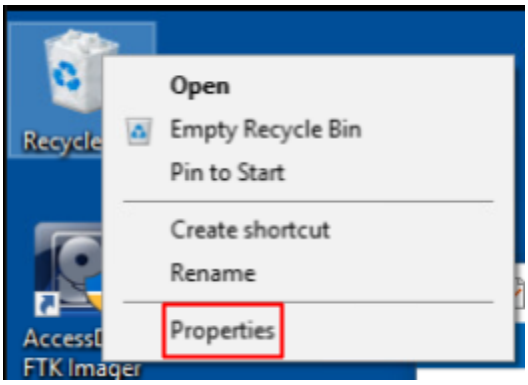
I then typed the following command:



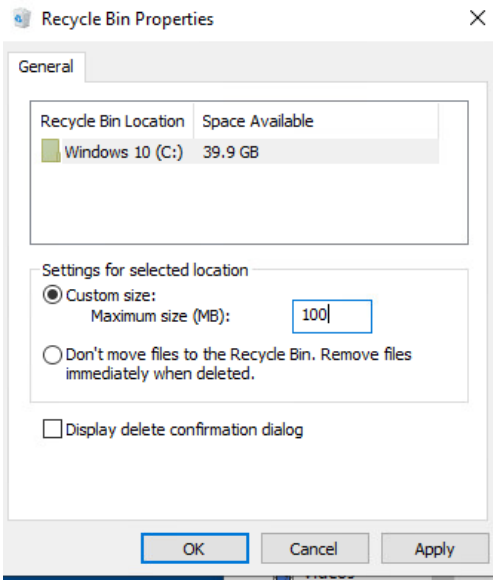
I took a screenshot of the results

5. **Change size of Recycle Bin**

   To change the size of the Recycle Bin, I right clicked the icon and selected “Properties”.

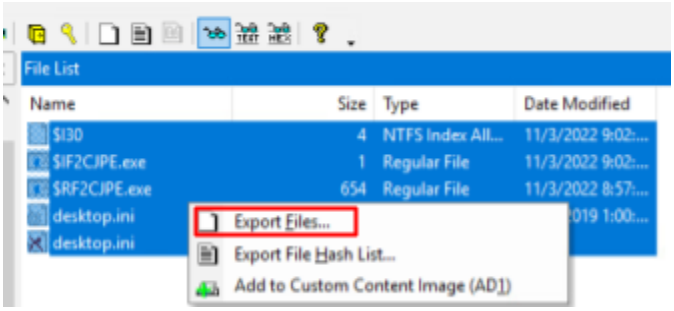


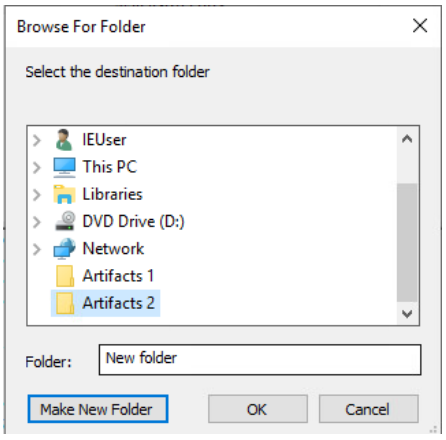
Next, I changed the number written in the box labeled Maximum Size (MB) from 4095 to 100. After the number was changed, I selected “Apply” then “OK”



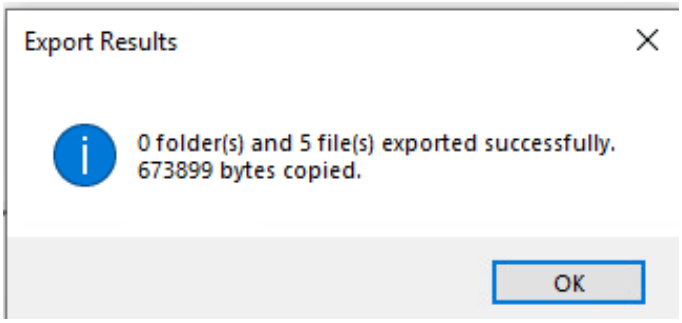
6. **Extract Files from FTK Imager**

Following the same steps above listed in Step 3, I exported the files to an Artifact 2 folder



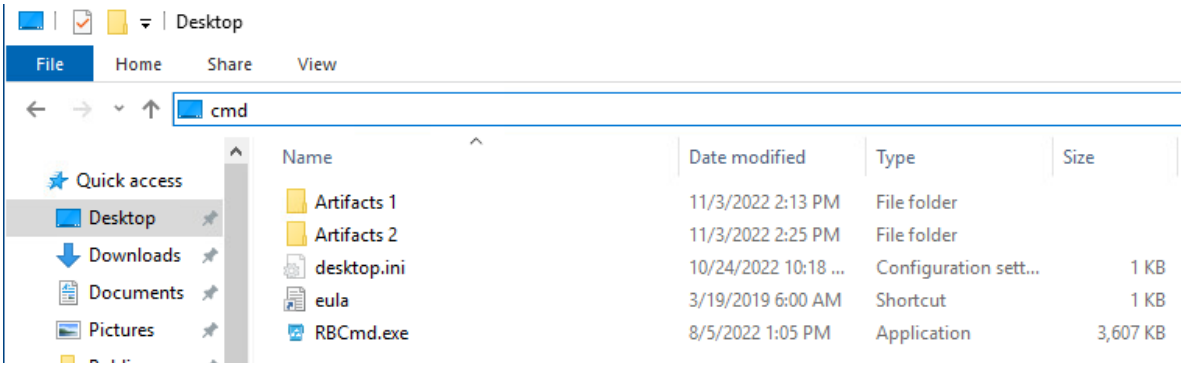


I received this confirmation:

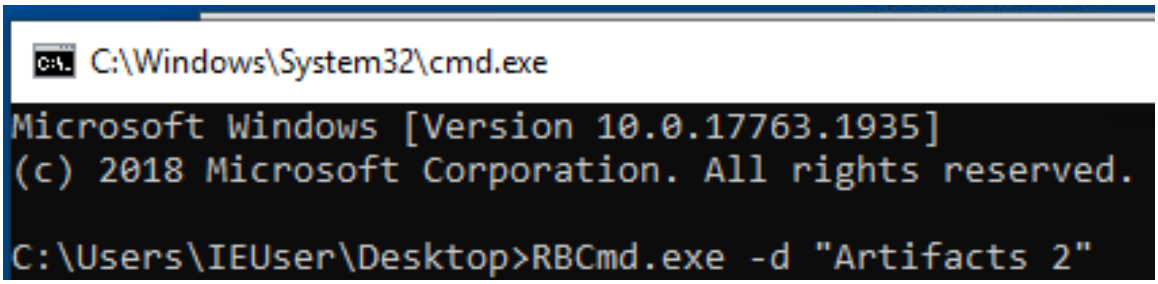


7. **Analyze the recovered files**
   Following the same steps listed in Step 4, I analyzed the contents of Artifacts 2.

   Type CMD into location bar:



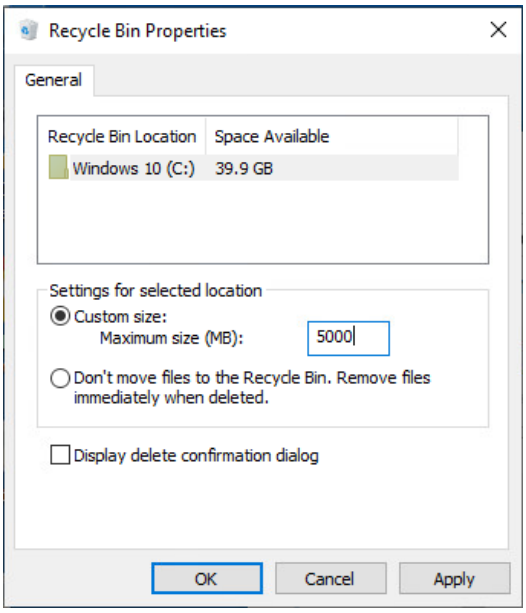
   Run the following command:



   I then took a screenshot of the results.

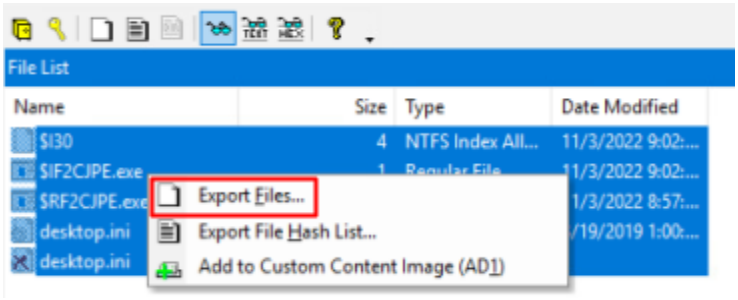
8. **Change size of Recycle Bin**

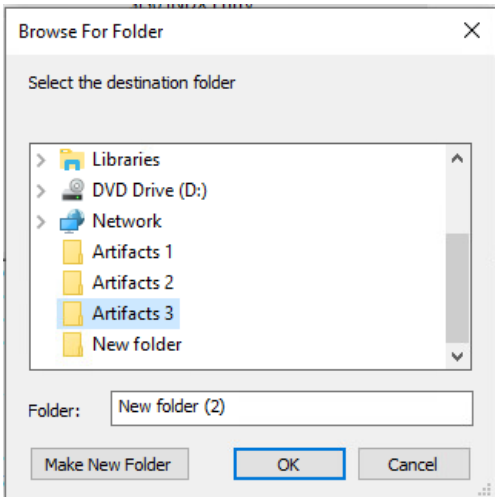
   Following the same steps listed in Step 5, I changed the size of the Recycle Bin from 100 MB to 5000 MB



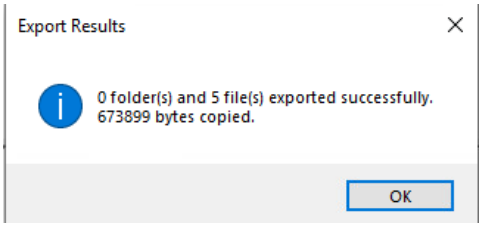
9. **Extract Files from FTK Imager**

   Following the same steps listed in Step 3, I exported the files to an Artifacts 3 folder.



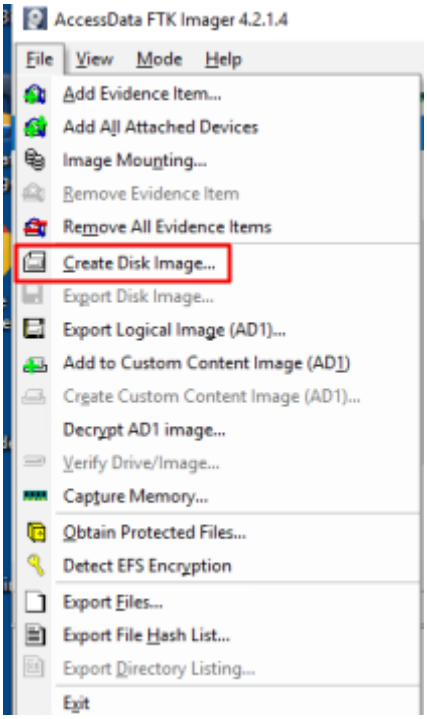


I received this confirmation:

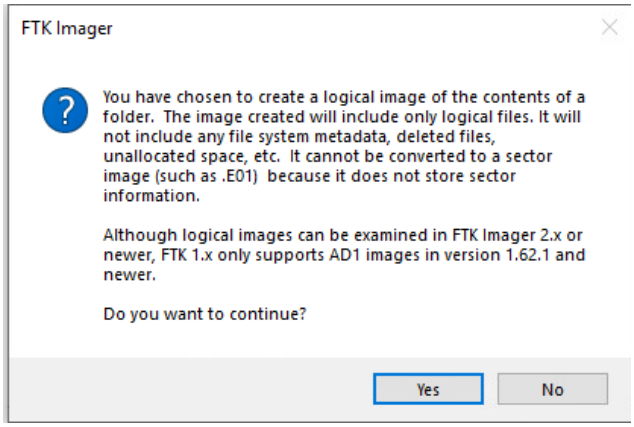


10. Make an Image

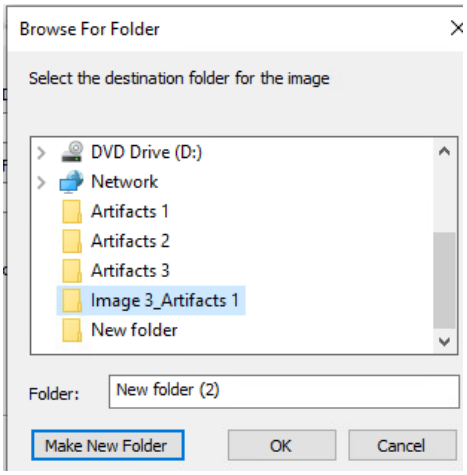
I used FTK Imager to make an image of each Artifacts folder by selecting "Create Disk Image".



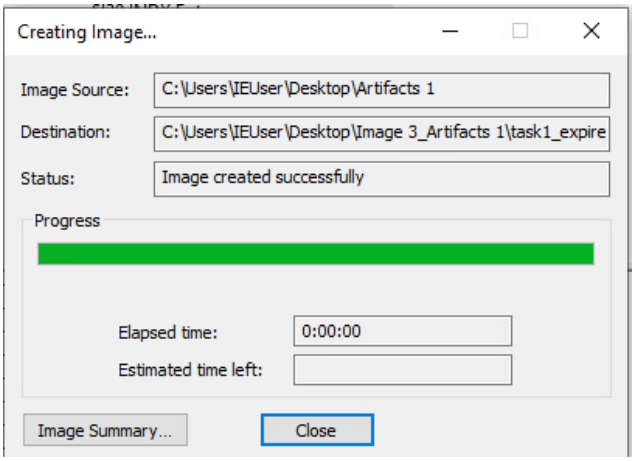
Next I selected Contents of a Folder and this confirmation popped up. I selected "Yes".

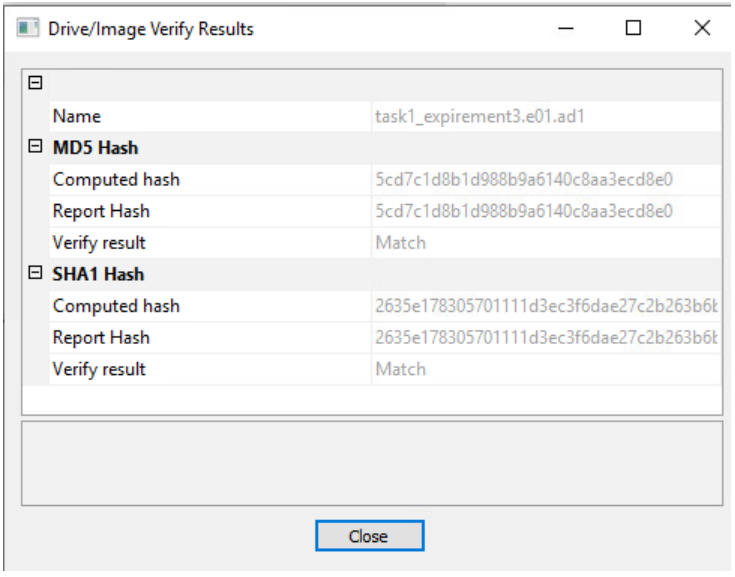


I selected the Artifacts 1 folder to image and exported the image to Image 3_Artifact 1 folder located C:\Users\IEUser\Desktop

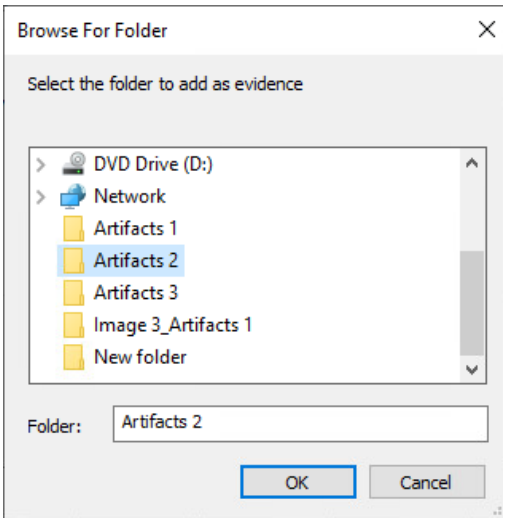


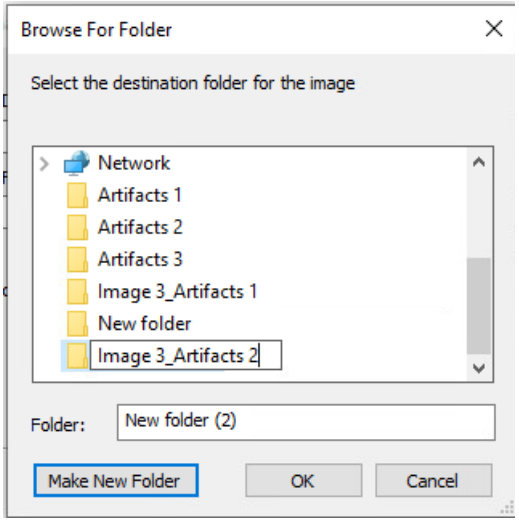
I received these confirmations:

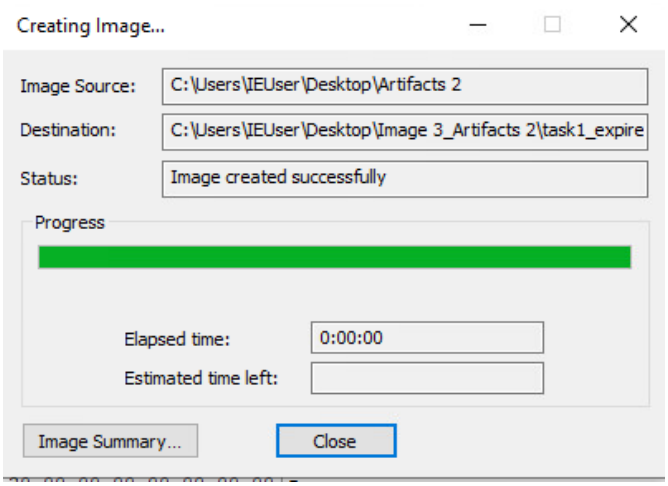


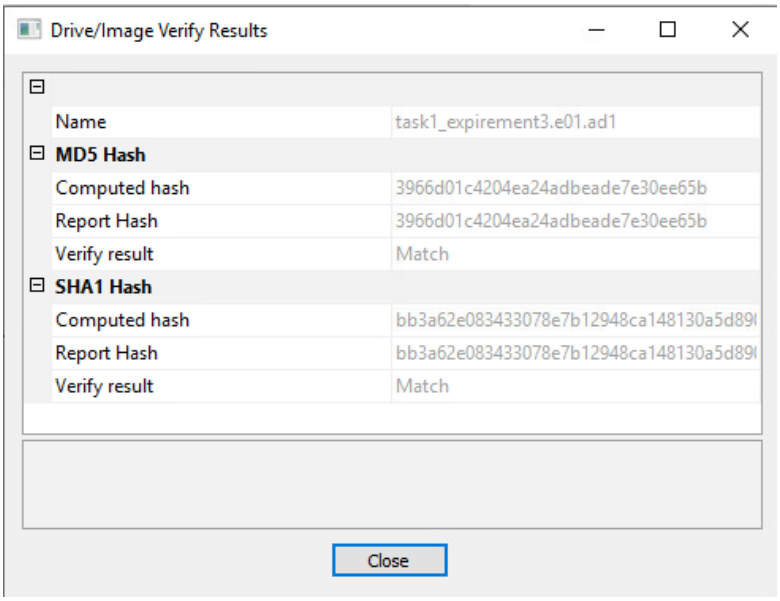


I repeated these steps for the Artifacts 2 and Artifacts 3 folders.
Artifacts 2:

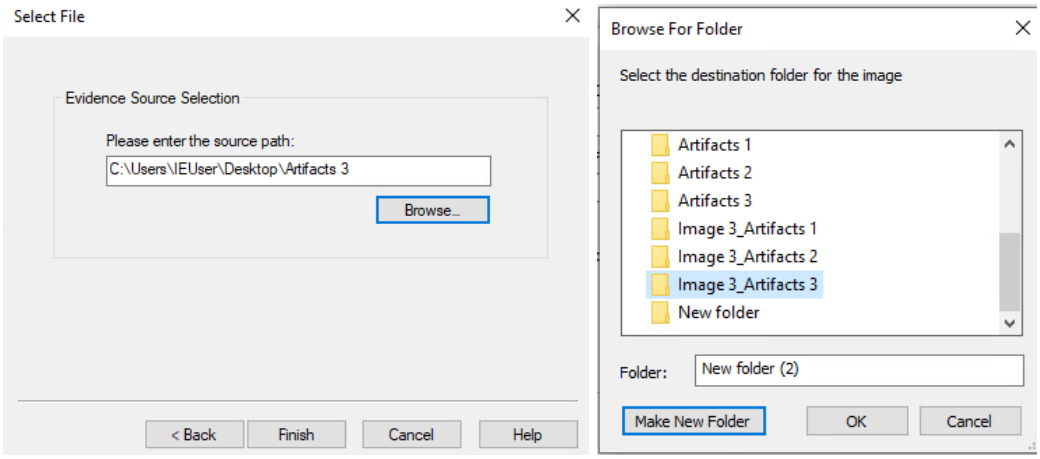


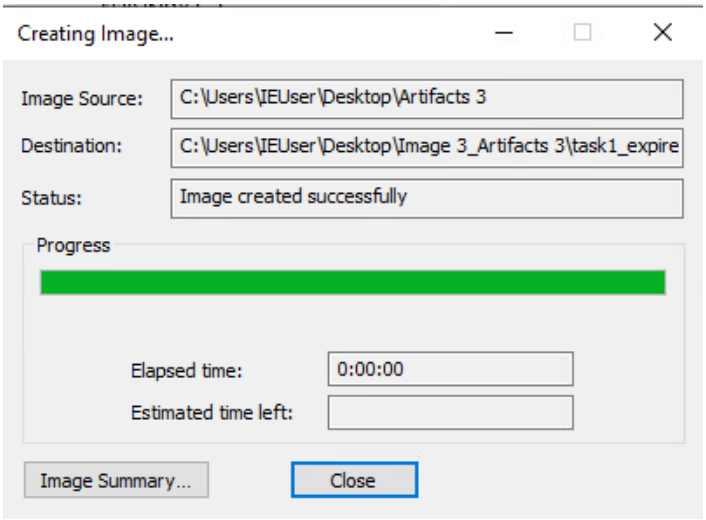


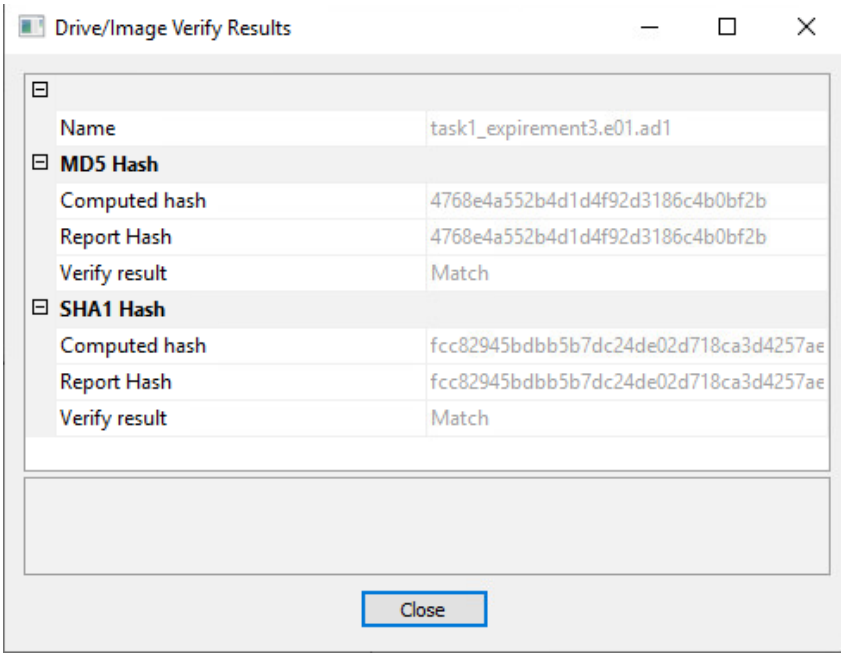




Artifacts 3:

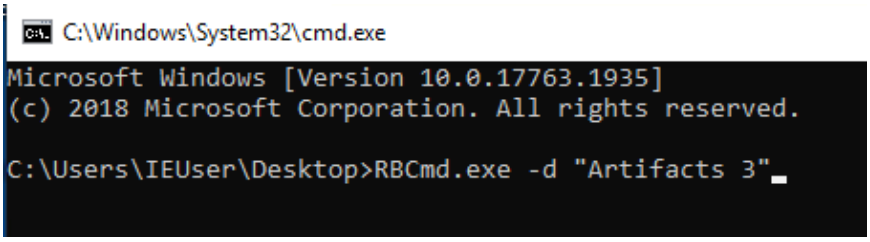

Select File
Evidence Source Selection
Please enter the source path:
C:\Users\IEUser\Desktop\Artifacts 3
Browse...
< Back
Finish
Cancel
Help
Browse For Folder
Select the destination folder for the image
Artifacts 1
Artifacts 2
Artifacts 3
Image 3_Artifacts 1
Image 3_Artifacts 2
Image 3_Artifacts 3
New folder
Folder:
New folder (2)
Make New Folder
OK
Cancel


Creating Image...
Image Source:
C:\Users\IEUser\Desktop\Artifacts 3
Destination:
C:\Users\IEUser\Desktop\Image 3_Artifacts 3\task1_expire
Status:
Image created successfully
Progress
Elapsed time:
0:00:00
Estimated time left:
Image Summary...
Close


Drive/Image Verify Results
Name
task1_expirement3.e01.ad1
MD5 Hash
Computed hash
4768e4a552b4d1d4f92d3186c4b0bf2b
Report Hash
4768e4a552b4d1d4f92d3186c4b0bf2b
Verify result
Match
SHA1 Hash
Computed hash
fcc82945bdbb5b7dc24de02d718ca3d4257ae
Report Hash
fcc82945bdbb5b7dc24de02d718ca3d4257ae
Verify result
Match
Close

11. Analyze the Recovered Files

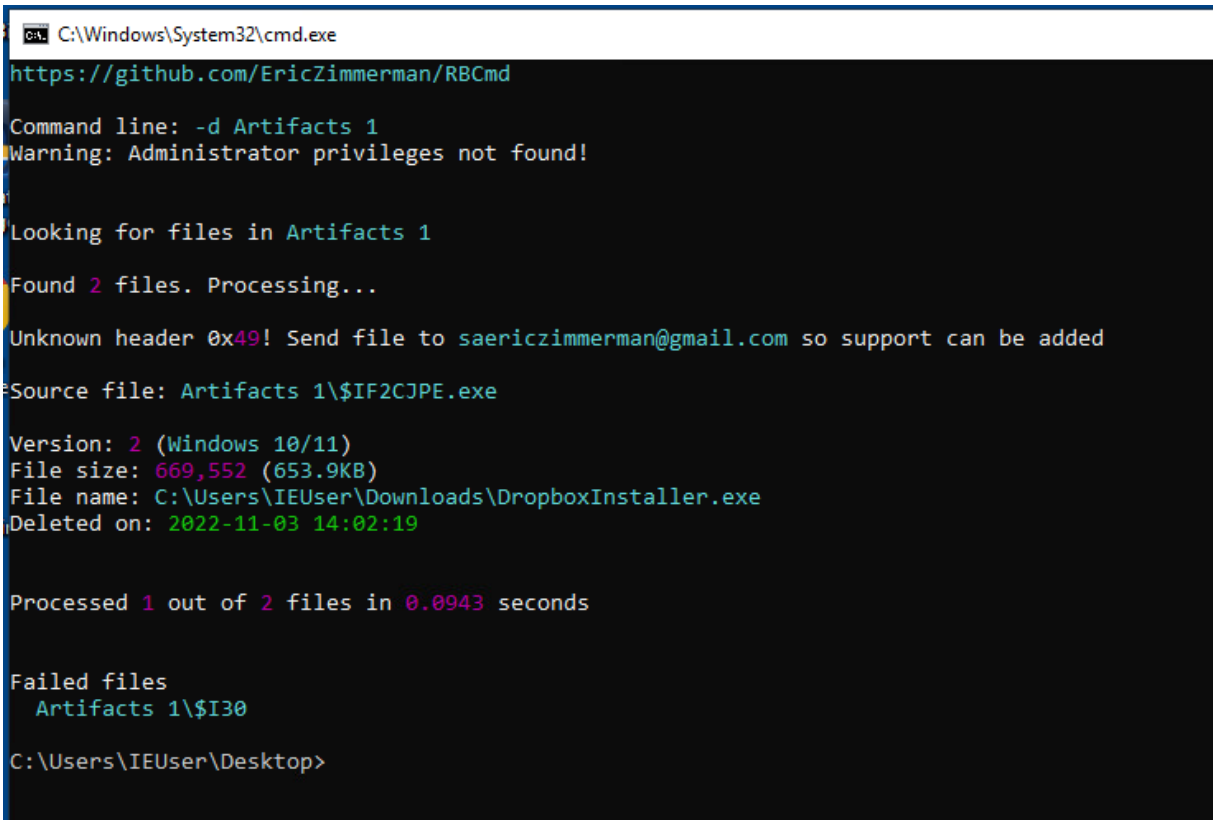
Following the same steps listed in Step 4, I analyzed the contents of Artifacts 3 and screenshotted my results.



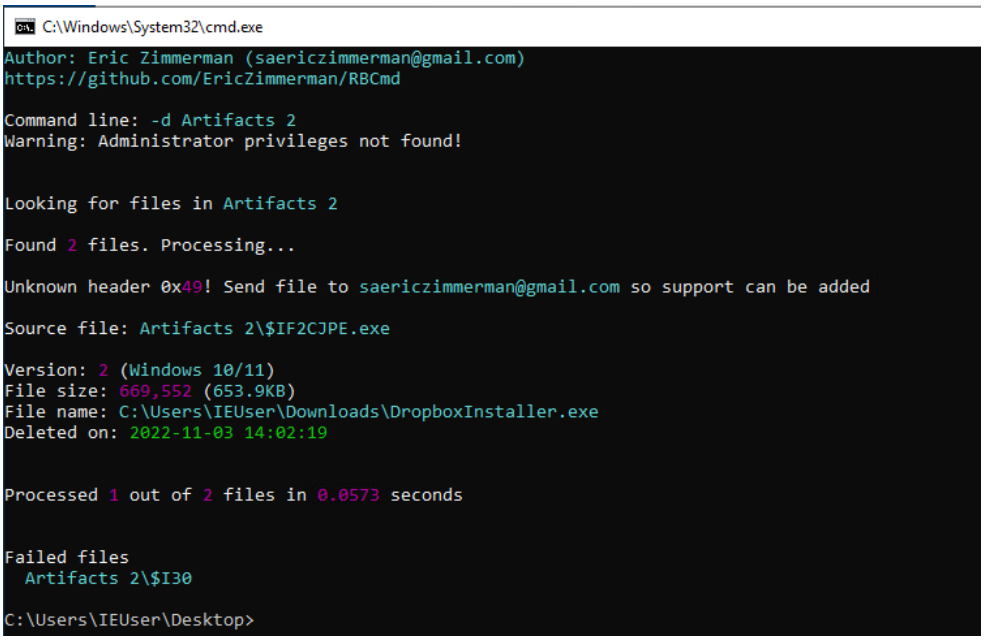
Results

When using RBCmd.exe to analyze the files located in my SID folder in $Recycle.Bin I received the following results:

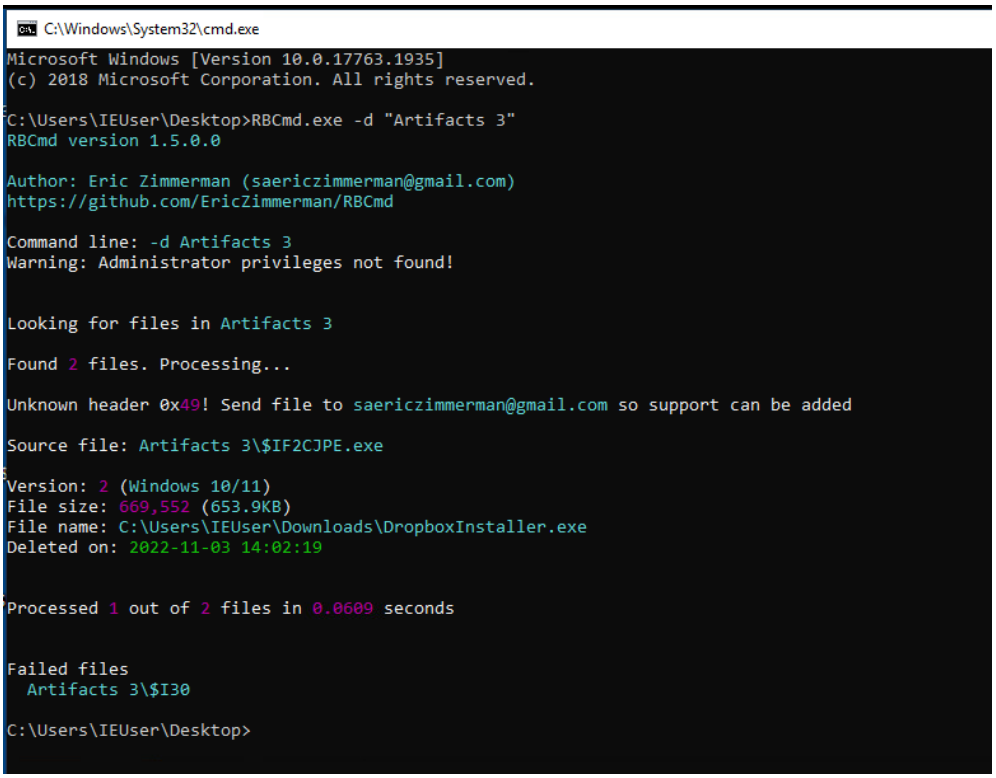
Artifacts 1:



Artifacts 2:



Artifacts 3:



RBCmd.exe successfully recovered metadata from $IF2CJPE in each Artifacts folder and failed to cover data from $I30. The contents of the $R files matched the contents of the file specified in RBCmd.exe

Analysis

The information that RBCmd.exe recovered from each folder was identical. Despite being three different folders, they had the same version, file size, file name, and deleted date. From these results we can infer that the content and metadata of a file remain unaffected by the allocated space of the Recycle Bin changing.

VI. Reflection

Changing the size of the Recycle Bin while a file is in it has no effect on its $I or $R files. The metadata located in the $I was still able to be extracted and showed no signs of being manipulated or altered.