By Rob Stewart

Digital Forensics CA3

Contents

[2 Introduction 2](#_Toc25417631)

[3 Tools Used 2](#_Toc25417632)

[4 Methodology 3](#_Toc25417633)

[4.1 Initial Setup 3](#_Toc25417634)

[4.2 Removing the files 5](#_Toc25417635)

[4.3 Image Acquisition 5](#_Toc25417636)

[4.4 Image Analysis 6](#_Toc25417637)

[4.4.1 Recycle Bin 6](#_Toc25417638)

[4.4.2 Documents Folder 7](#_Toc25417639)

[4.4.3 Shift + Delete 8](#_Toc25417640)

[4.4.4 Cut and Paste to USB 11](#_Toc25417641)

[4.4.5 Del in command line 12](#_Toc25417642)

[4.4.6 Erase in command line 12](#_Toc25417643)

[4.4.7 Possible evidence of all removed images 13](#_Toc25417644)

[5 Conclusion 16](#_Toc25417645)

# Introduction

The purpose of this report is to analyse the forensic significance of the multiple options that the user can use to remove files from a Windows 10 system, how effective each removal method will be researched and analysed.

The following options were examined:

1. Select the file and click delete button on the keyboard
2. Select the file and click the shift and delete buttons on the keyboard
3. Cutting and pasting the file to a removable disk
4. Dragging the file to the Recycle Bin
5. Del in command line
6. Erase in command line

# Tools Used

The following tools were used during the investigation:

1. Windows 10 Education, 64-bit Desktop PC
2. Oracle VirtualBox Version 6.0.14 r133895 (Qt5.6.2) with VirtualBox Extension Pack
3. Autopsy Version 4.12 (64-bit)
4. USB 2GB

# Methodology

## Initial Setup

A windows 10, 64-bit virtual machine (VM) was created within VirtualBox. The basic settings for this VM can be seen in Figure 4‑1

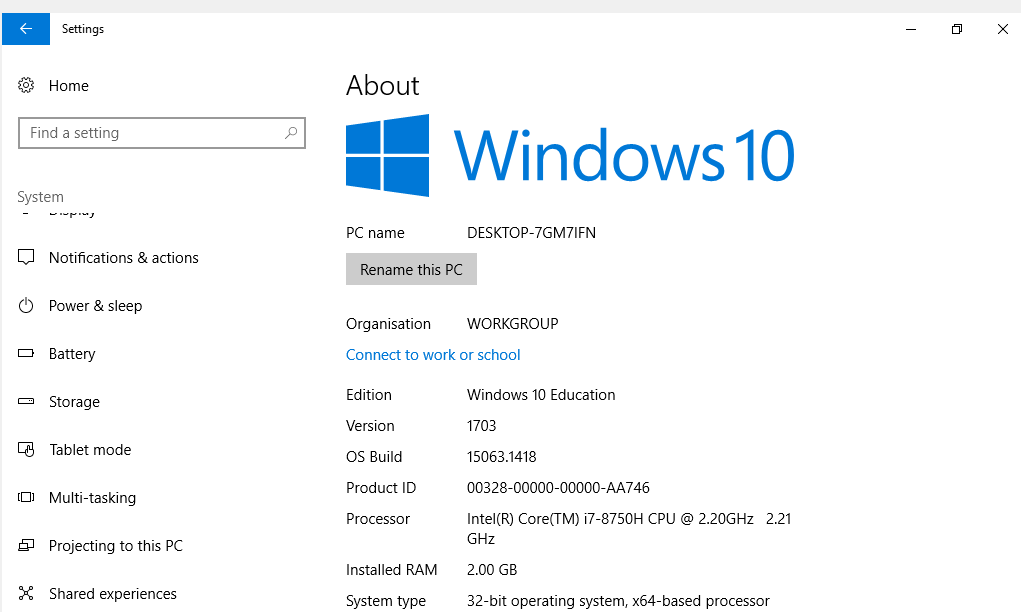


Figure ‑ vm settings

10 files of various types were added to a USB key to be copied to the Windows system. The files can be seen in Figure 4‑2.

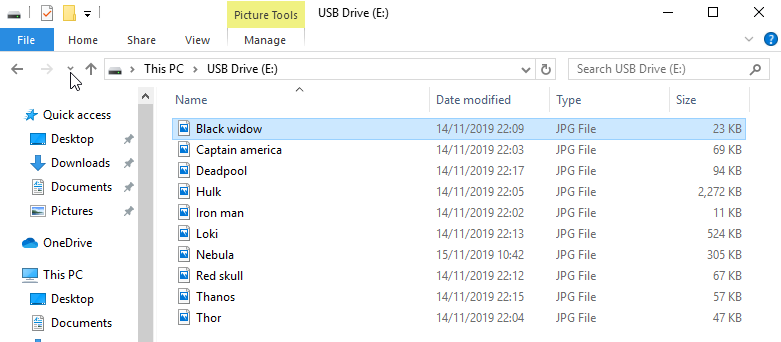


Figure ‑ Files on USB key

The USB key was added to the VM and the files were then copied to the Documents folder on the Windows 10 system as shown in Figure 4‑3.

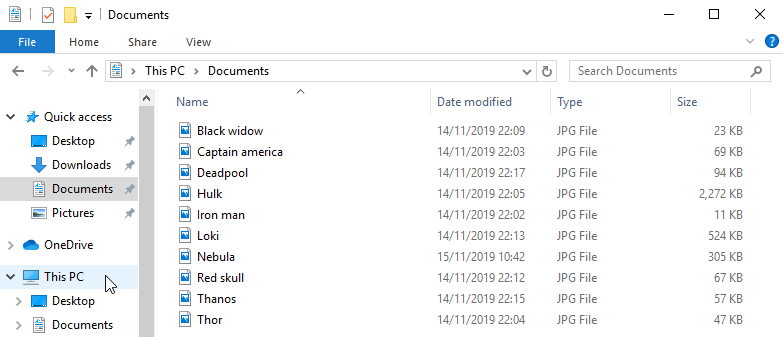


Figure ‑ Files in Documents folder

## Removing the files

The files were removed according to Table 4‑1

|  |  |  |
| --- | --- | --- |
| File Number | File Name | Removal Method |
| 1 | Black Widow.jpg | Delete button on Keyboard |
| 2 | Captain America .jpg | Shift and Delete on Keyboard |
| 3 | Deadpool.jpg | Cut and Paste to USB |
| 4 | Hulk.jpg | Dragged to Recycle Bin |
| 5 | Ironman.jpg | Del in command line |
| 6 | Loki.jpg | Erase in command line |
| 7 | Nebula.jpg | Cut and Paste to USB |
| 8 | Red Skull.jpg | Shift and Delete on Keyboard |
| 9 | Thanos.jpg | Not Removed |
| 10 | Thor.jpg | Not Removed |

Table ‑ Methods used to remove each file

## Image Acquisition

Once the files were removed the vm was shutdown normally to obtain a post – mortem image. The VBoxManage part of VirtualBox was used to obtain the image. The UUID of the vm was found to be a60f0f86-5641-4c89-bf14-435d0763764c and the location of the .vdi file was E:\Users\Sky\VirtualBox VMs\Windows 10 NTFS\Windows 10 NTFS.vdi

Using this information, a raw image of the vm was obtained as shown in Figure 4‑4

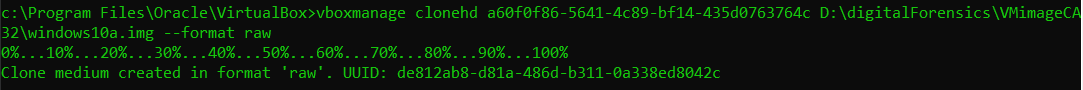


Figure ‑Image creation process

## Image Analysis

The raw image was examined using Autopsy. The first area to be examined was the Recycle Bin as shown in Figure 4‑5

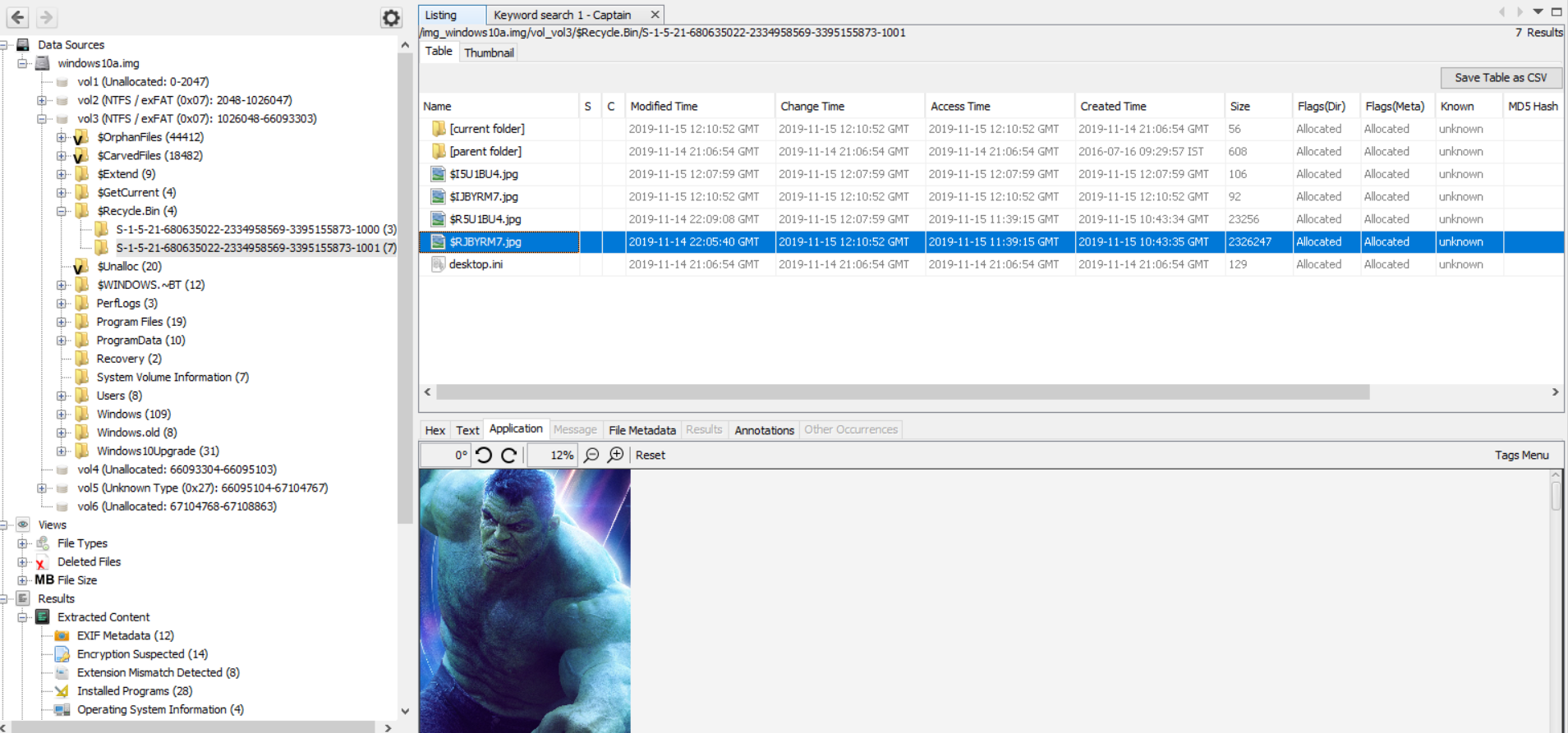


Figure ‑ Contents of Recycle Bin

### Recycle Bin

When a file is added to the Recycle Bin, 2 files are added to the folder. An I file and an R file is created. Both files have the same random 6-digit filename. They also have the original extension of the file added to the Recycle Bin. The first file in Figure 4‑5 is $I5U1BU4.jpg has a matching R file, $I5U1BU4.jpg. The $I file indicates the original filename and location C:\Users\rob\Documents\Black Widow.jpg. According to Table 4‑1, this file was removed using the delete button on the keyboard. Table 4‑2 documents the $I and $R files found in the Recycle Bin. From this table it is possible to determine that files dragged to the recycle Bin or Deleted using the delete key are added to the Recycle Bin.

|  |  |  |  |
| --- | --- | --- | --- |
| I$ | $R | Filename | Removal Method |
| $I5U1BU4.jpg | $R5U1BU4.jpg | Black Widow.jpg | Delete button on keyboard |
| $IJBYRM7.jpg | $RJBYRM7.jpg | Hulk.jpg | Dragged to Recycle Bin |

Table ‑ Files found in Recycle Bin

### Documents Folder

The only files that remain in the Documents folder are the 2 files that were not removed, Thanos.jpg and Thor.jpg seen in figure 4-6, the deleted files should be here and the additional deleted Thor file should not be there, the only evidence of the other files exists in the meta data.

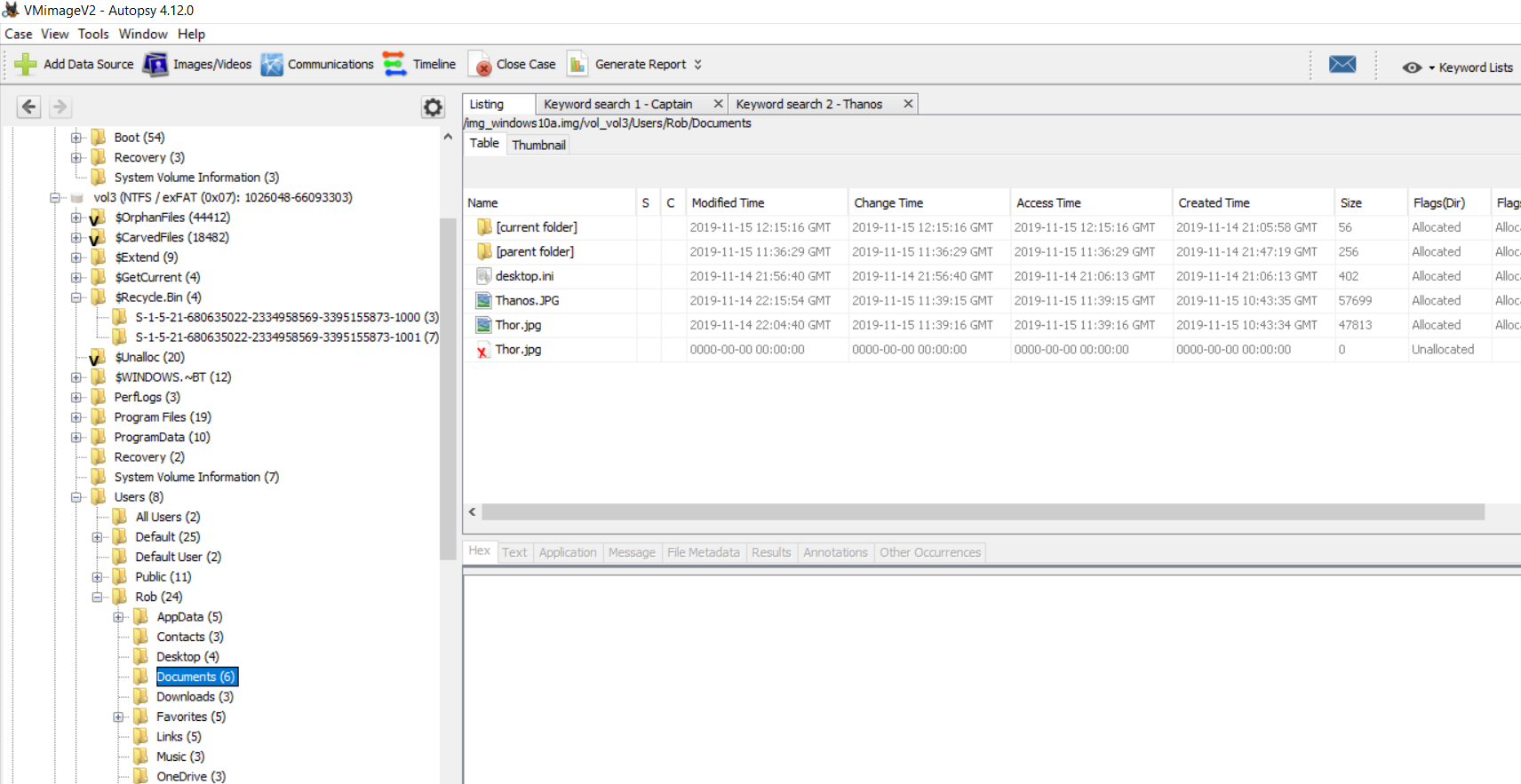


Figure ‑6 Contents of Recycle Bin

### Shift + Delete

A keyword search for the string Captain returned the results as shown in 4-7.

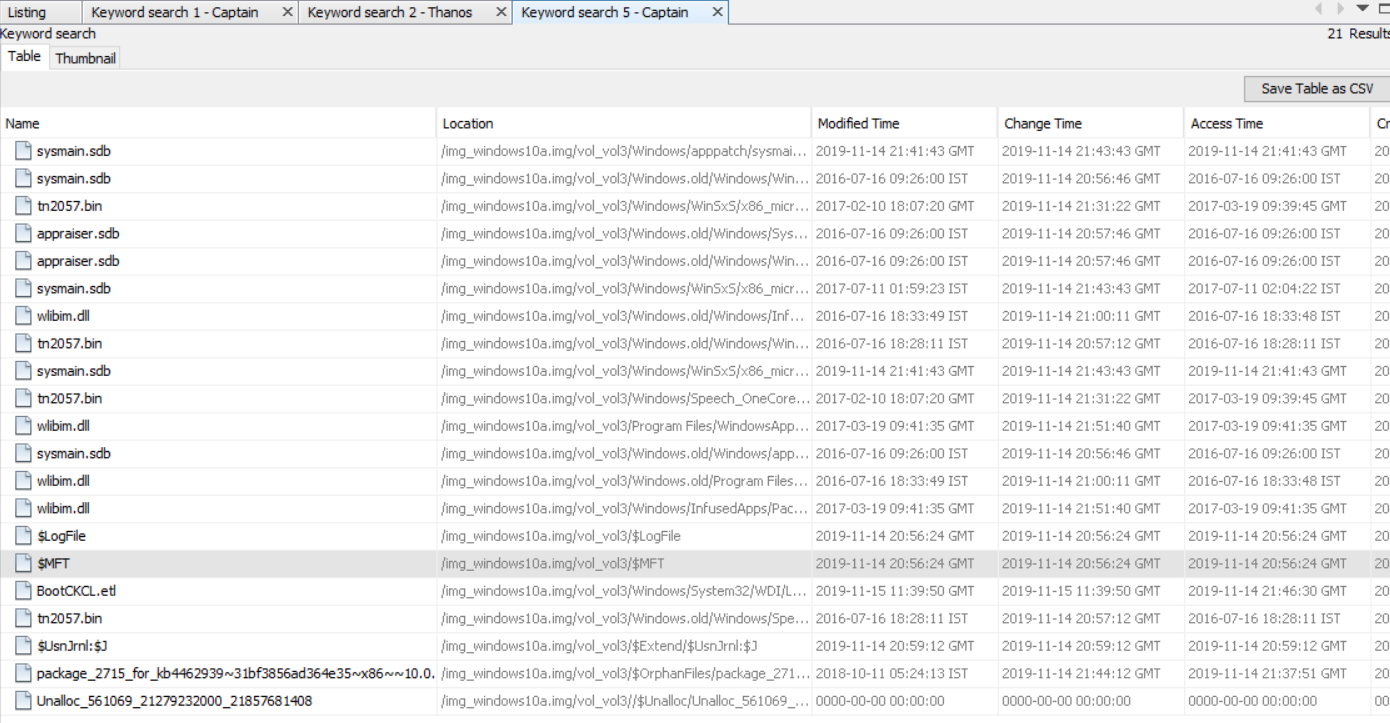


Figure ‑7 Keyword search "Captain"

The following 5 highlighted files are to only files from the above screenshot that contain information on the Captain America.jpg image.

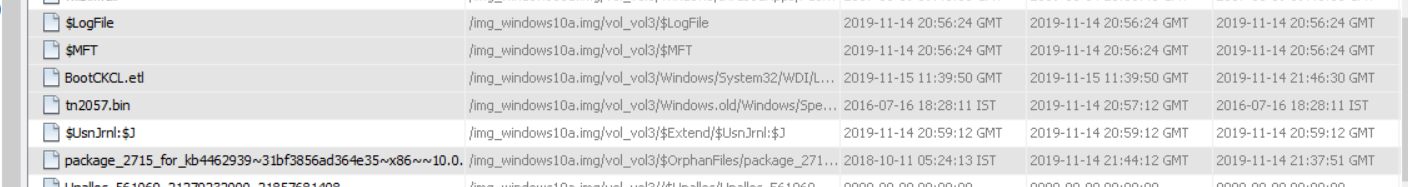


Figure ‑8 Files that contain the jpg image.

On opening the log file a record of the Captain America.jpg was discovered.

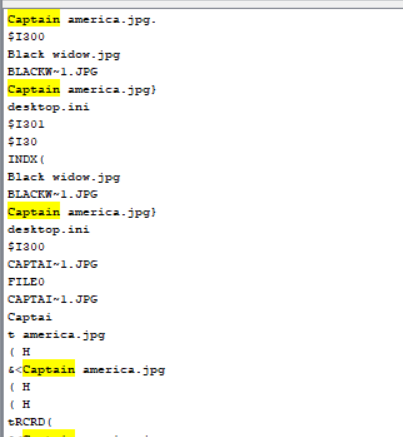


Figure ‑9 Evidence of image.

On further investigation in the log file, evidence of all the images was discovered no approach for delete indefinitely removed evidence of any of the images.

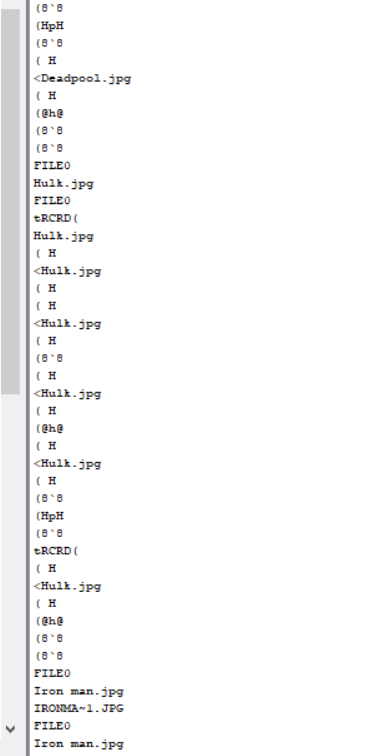


Figure ‑10 Evidence of all images.

Below shows the image in the $MFT folder.

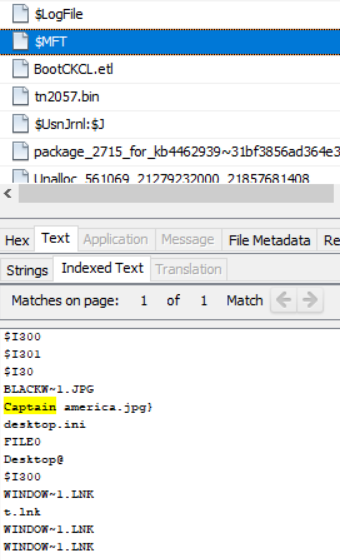


Figure ‑11 Image in $MFT file.

In the bootCKCL.etl the image is shown to be present on the Harddisk Volume four on the virtual machines hard drive.

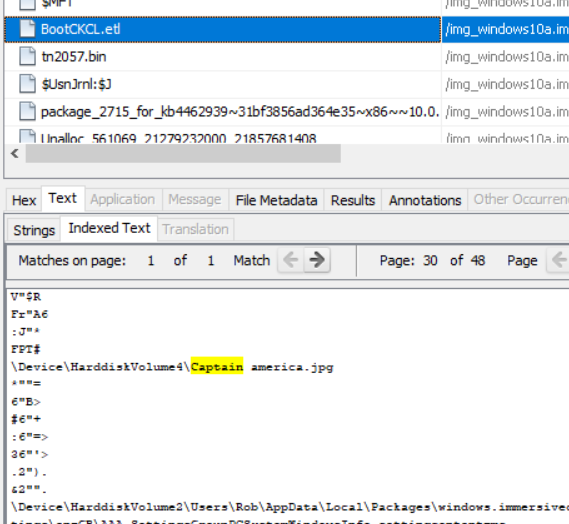


Figure ‑12 Image present on harddisk.

Further investigation on the Harddisk Volume 4 shows that there is nothing indexed on it, proving that the image exists on the hard drive in unallocated space.

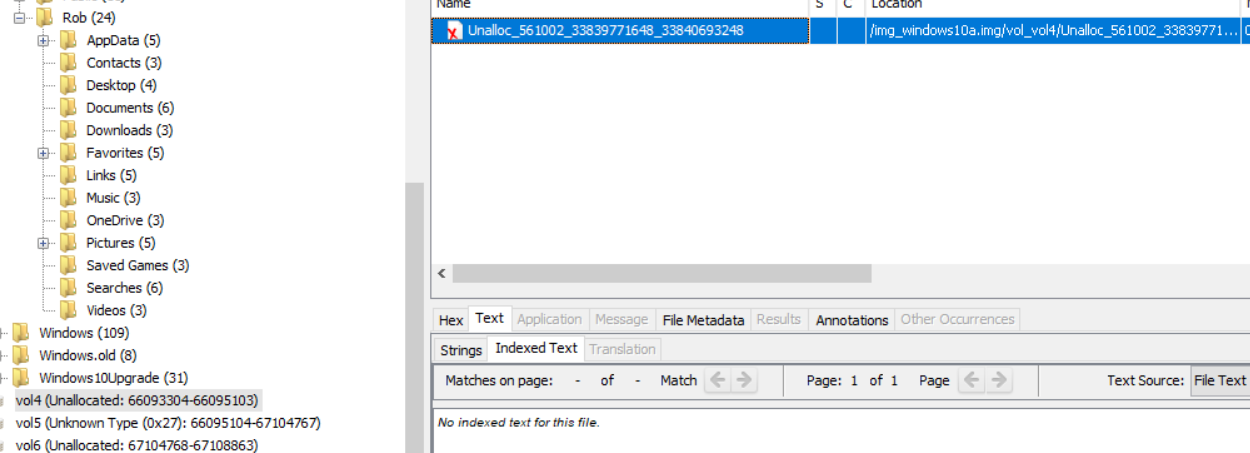


Figure ‑13 Image not indexed on hard drive.

### Cut and Paste to USB

This image lacks a $MTF and Log file, only meta data relating to image can be found and unallocated space on Volume 3 references it.

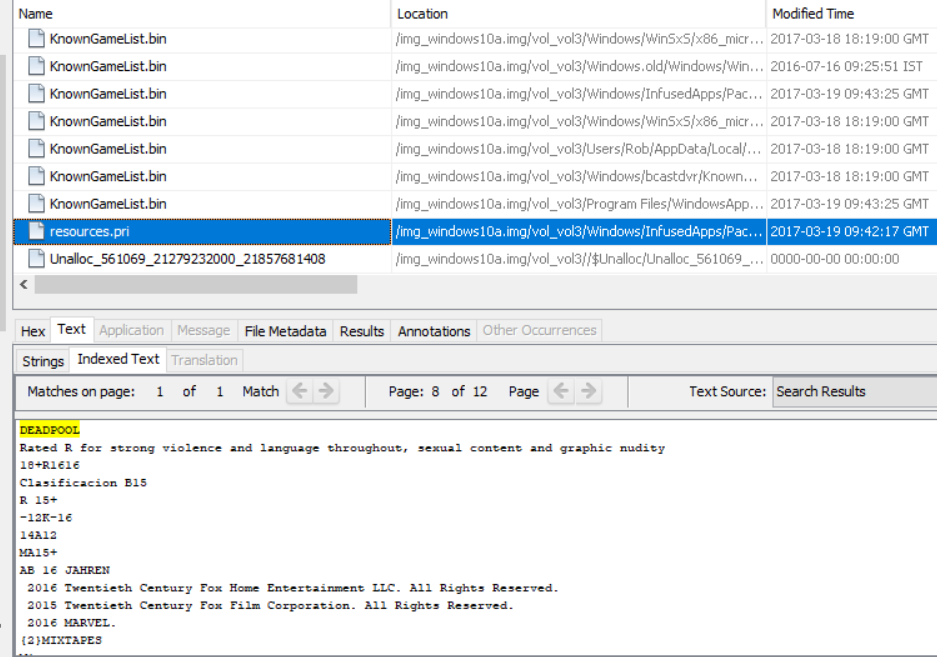


Figure ‑14 Image lacks a Log file or $MTF record.

### Del in command line

This method of deletion is the most effective as it shows zero results for the Ironman.jpg, the only evidence found of its existence is in the log file for the Captain America.jpg search found in figure 4-10, using this function on all images would prove to be the most effective.

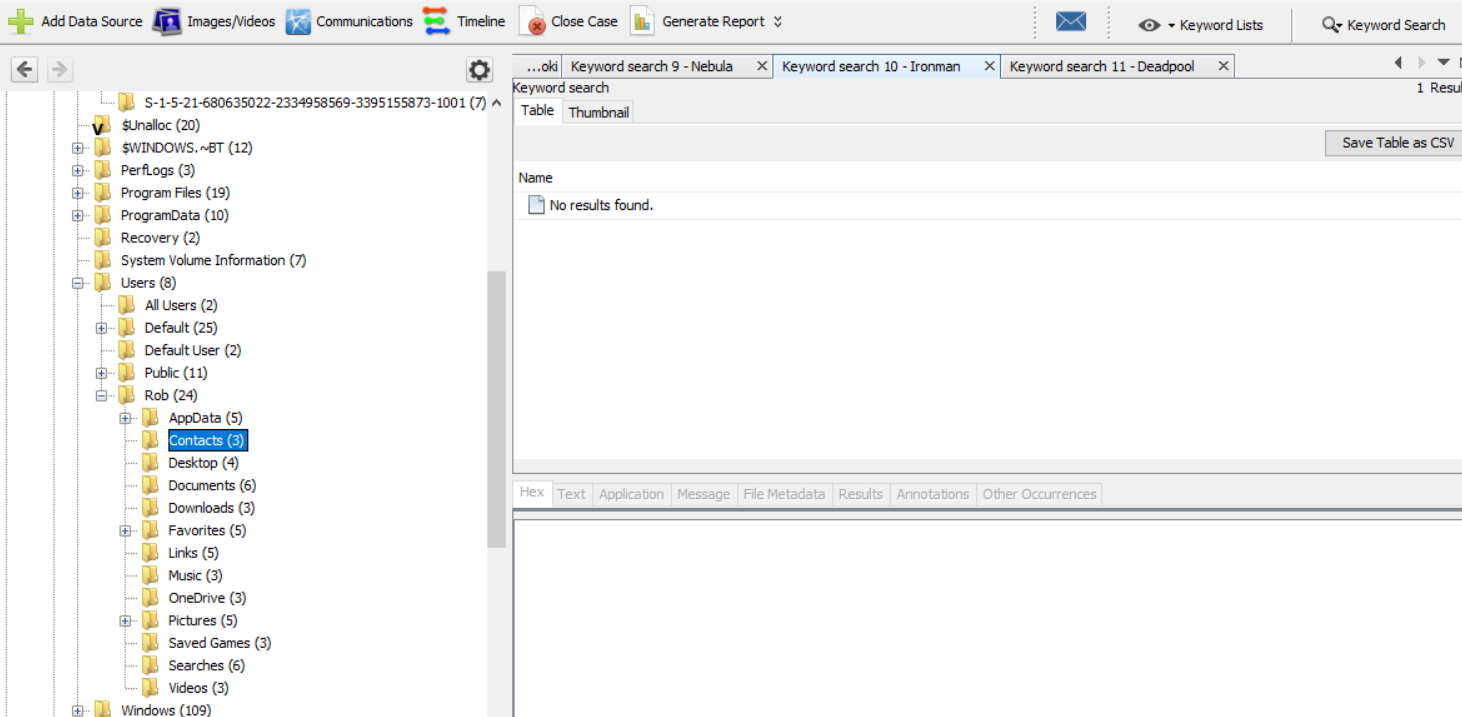


Figure ‑15 No results found for Ironman.jpg.

### Erase in command line

Erase seems to have the same effect as Del in regards to the image, a lot of results were found on the key word search but none relate to image at all, only evidence is again in the log file in Figure 4-10.

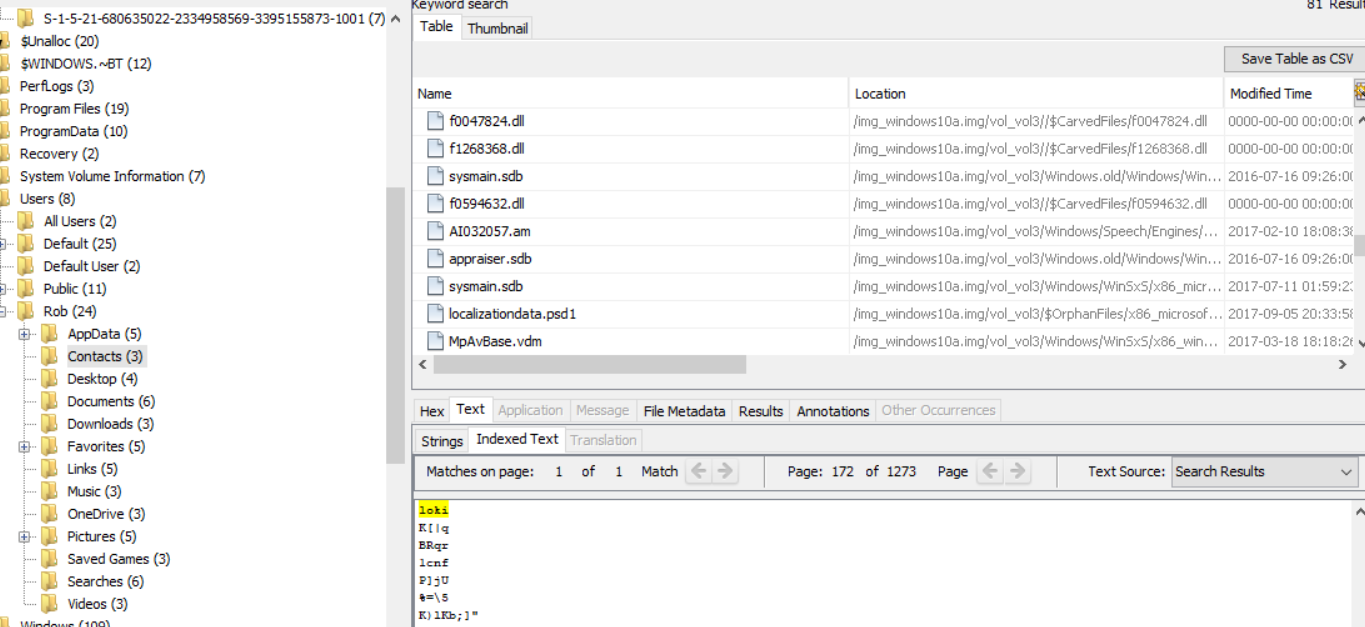


Figure ‑16 No results found for Loki.jpg

### Possible evidence of all removed images

In Figure 4-14 the eight highlighted unallocated files seem to have a correlation with the eight deleted images, including the two that were moved to the recycle bin. This shows evidence that in the case of the two recycle bin images, they also exist in their original hard drive space in unallocated form. Additionally this exists on volume 3 instead of volume 4.

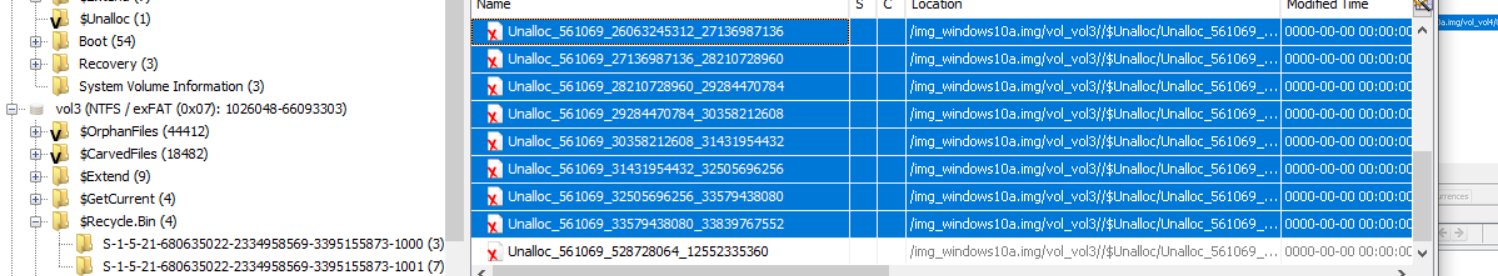


Figure ‑17 Evidence of all eight files.

Files have been overwritten with the new images added to the Documents directory, this proves the unallocated space has been allocated to the new files, unfortunately the visible evidence is the deleted Thor file is no longer visible.

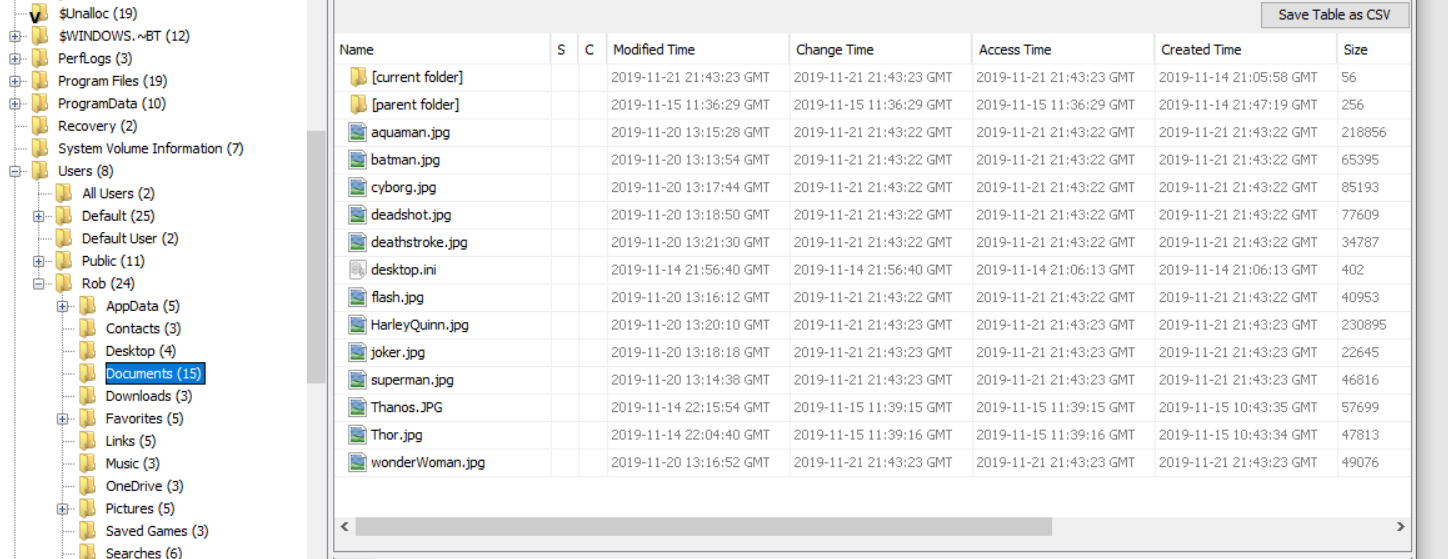


Figure 4‑18 New files added to documents.

The MFT record shows that the previous files where once on the system, but recovering them would be extremely difficult now the unallocated space they were written to, has be allocated to the new images.

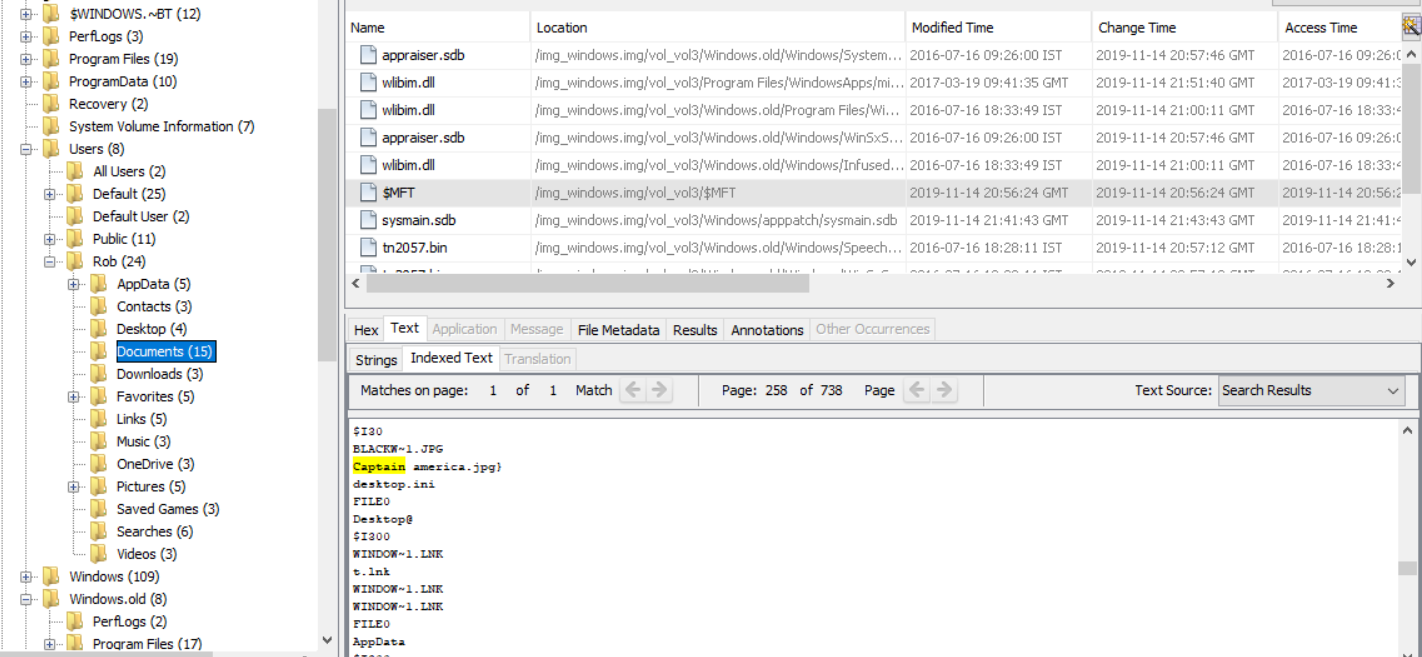


Figure 4‑19 MFT record of original images

An image of the USB holding the database from MONDIAL.ltd was acquired

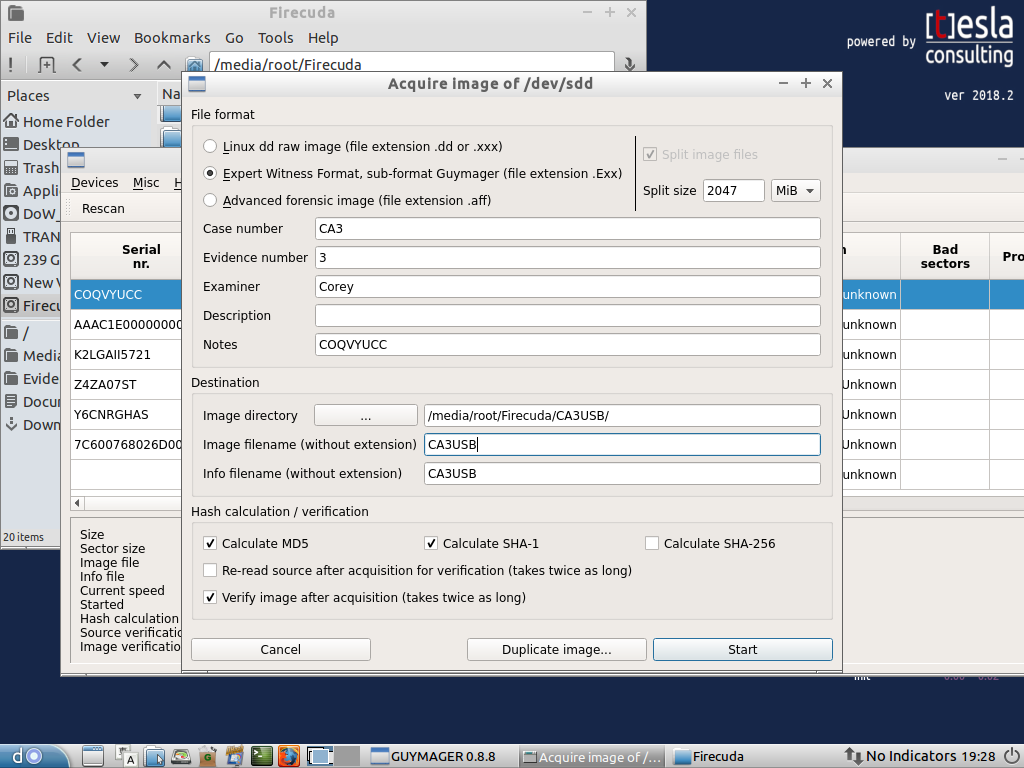


Figure 4‑20 Image acquisition of the USB.

The deleted database is still present on in the unallocated space on the USB drive.

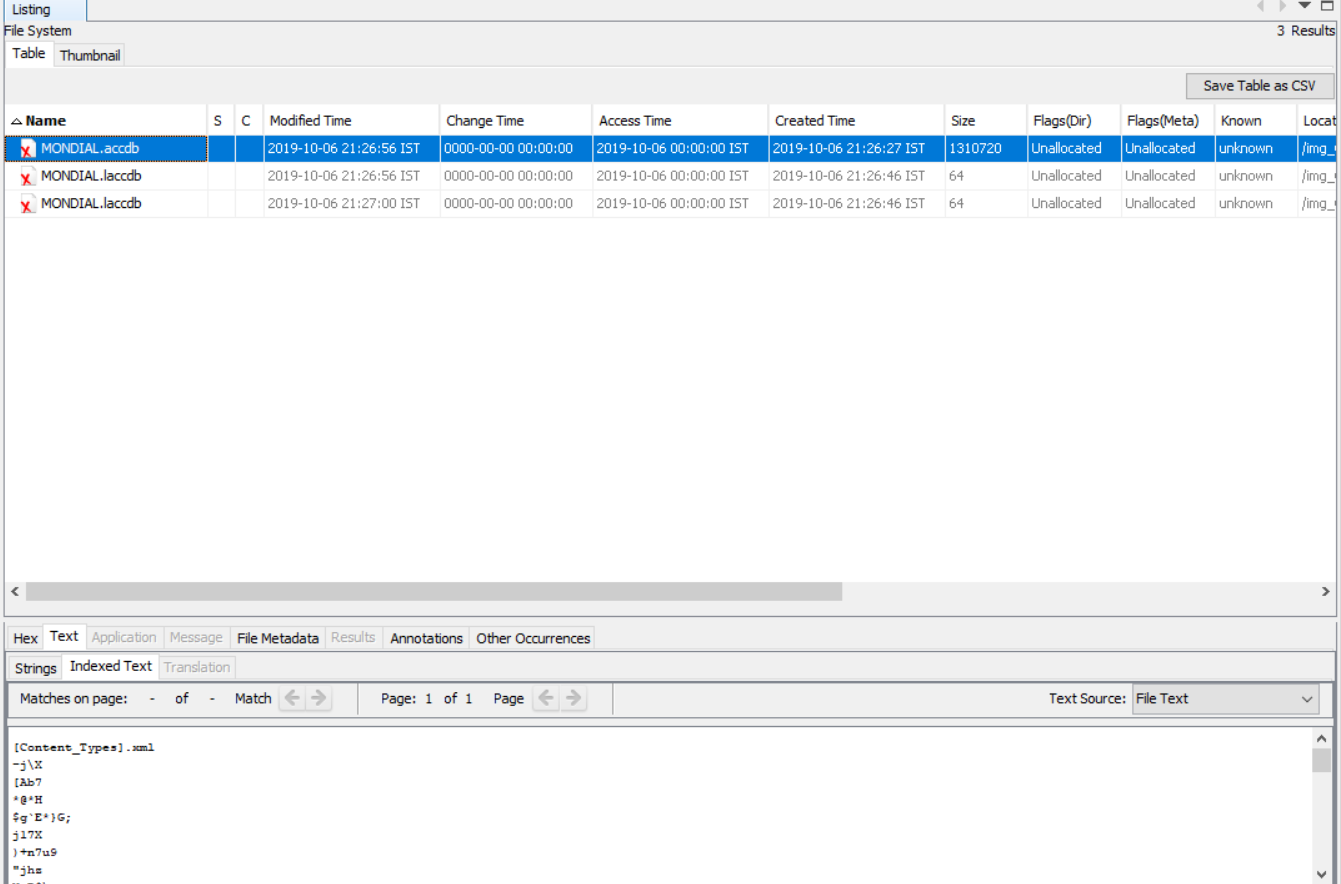


Figure 4‑21 Database in unallocated space.

After writing a new file to the USB and acquiring another image, it is showing that the database has been overwritten by the new file.

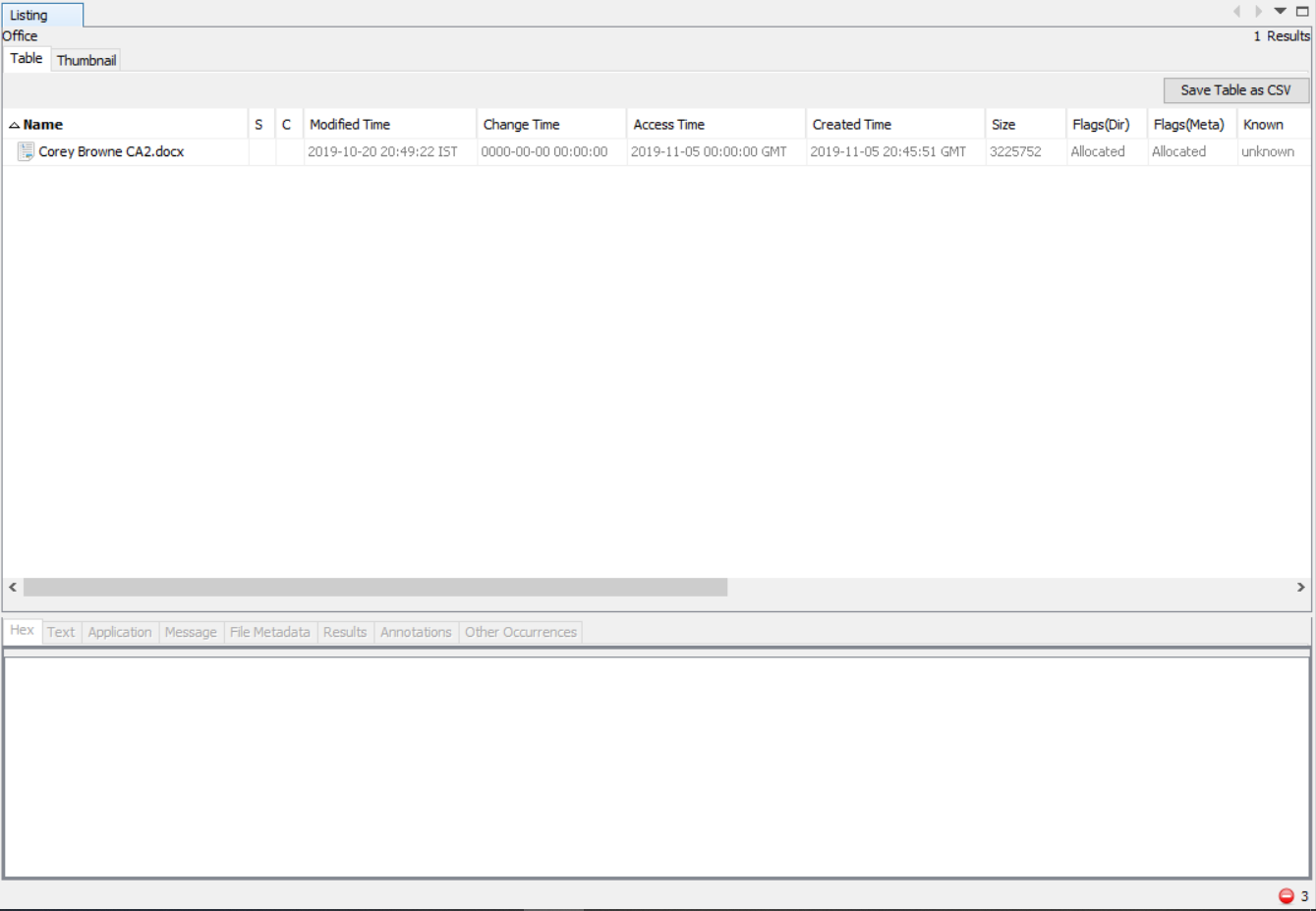


Figure 4‑22 Database overwritten by new file.

Attempting to extract an reopen the database is pointless as Microsoft Access cannot recognise the new contents in the allocated space.

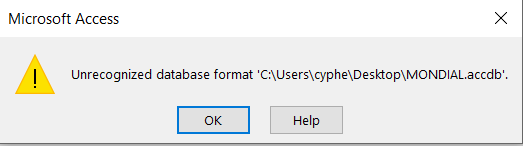
.

Figure 4‑23 Database cannot be opened.s

# Conclusion

Amongst all the tested deletion methods using the Del and Erase in command line prove to be the most effective, they are however not perfect records of items deleted through command line can be found in MTF and Log files within other deleted documents. Shift and delete while it was effective at removing a record from the recycle bin, it still produced MTF and Log files, the same is true for cut and paste to a USB.

The absence of all files in unallocated space, except for the Thor.jpg which also was never deleted, is unknown, unallocated files were found on a different Volume which seem to correlate with the eight deleted files, but direct relation is unconfirmed. The use of command line may have altered unallocated space records for all deleted files.

Drag to Recycle Bin and Delete on the keyboard proved the least effective allowing forensic tools to easily view the content in the Recycle Bin, furthermore a user can easily access the Recycle Bin through the Windows 10 operating system and retrieve all contents if it hasn’t been emptied.

Main point to take away is that a user who is proficient at using command line will hide their activity better than others.

The systems don’t move to the next piece of designated free space in these examples, anytime a file is deleted and goes into unallocated space, the next file written in goes into the space the older file was sitting in, instead of moving past it. This isn’t a guarantee but seems to be the most recurring outcome.

In NTFS recovering the deleted files is easier than in a FAT file system, NTFS indexes the files where as FAT does not.