RAMADHAN BERBAGI #1

FORENSICS OF WINDOWS RECYCLE BIN

Izazi Mubarok

Digitally signed by Izazi Mubarok
Date: 2020-04-26 06:34+07:00

Overview

- How to delete a file in Windows?
  - Send file to Recycle Bin
  - Delete file from File system
- How to recover a file deleted in Windows?
  - File system Recovery (Restore)
  - Data Carving
- Forensics of Recycle Bin
  - Location, folder structure, and content of Windows Recycle bin
  - $I… files

Delete a file in Windows

- Drag and drop file into Recycle Bin
- Select file, press “Delete” key
- Select file, right-click, select “Delete” option
- Select file, press “Shift” and “Delete” keys
- Select file, right-click, press “Shift” key and select “Delete” option
- Delete file from command line

Send to Recycle Bin

- Drag and drop file into Recycle Bin
- Select file, press “Delete” key
- Select file, right-click, select “Delete” option

Delete file from the file system

- “Shift” and “Delete”
- Delete file from command line

File Recycling

- Not permanently deleted
- Renamed and moved to a hidden folder
- Can be restored to its original name and location

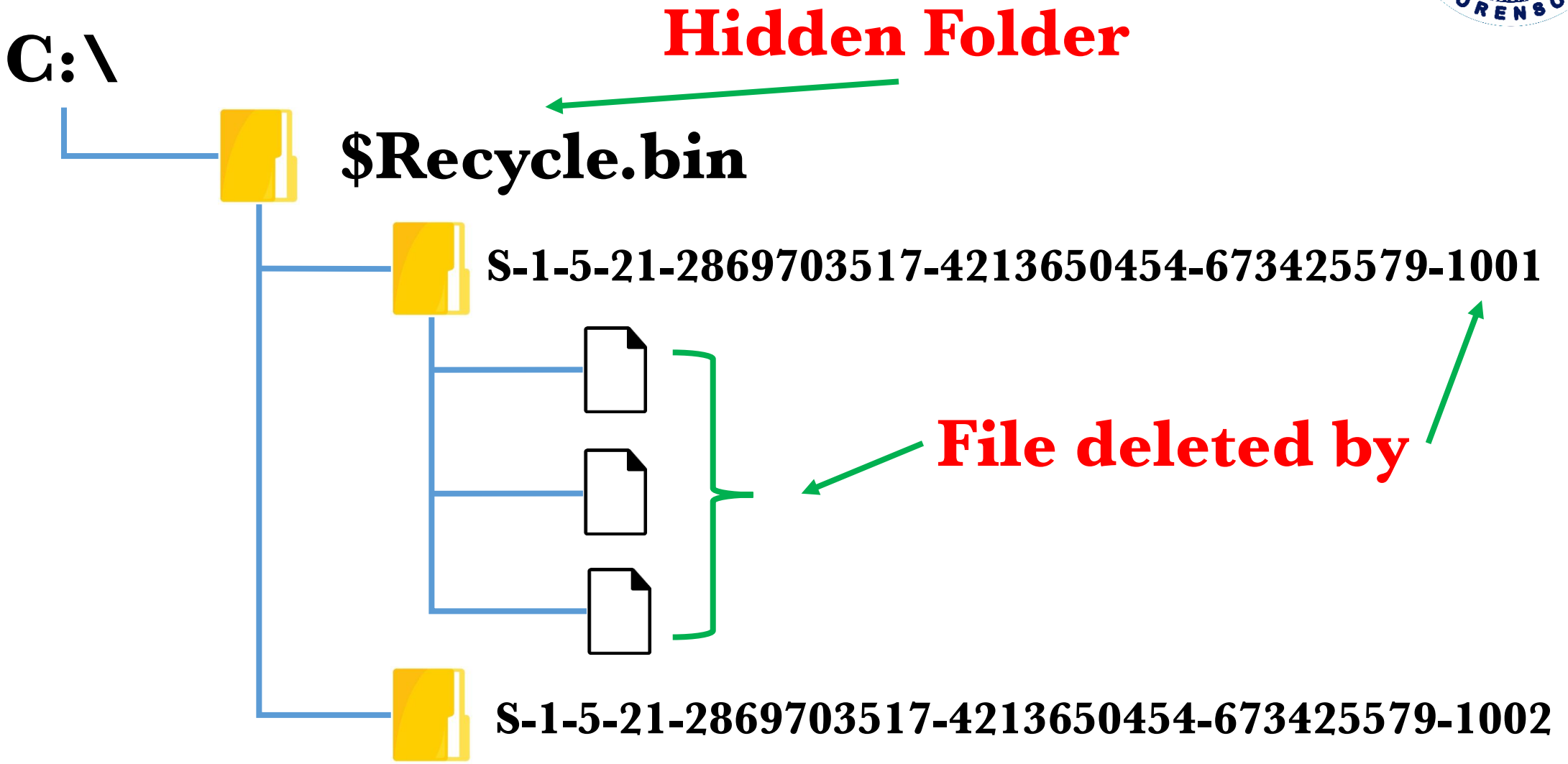
Forensics of Recycle Bin

- Files are moved into Recycle Bin by explicit command from the user
- Presence of a file/folder in the Recycle Bin usually indicates
  - user awareness of the file/folder
  - intent to remove it

Folder Structure

- Each logical drive has hidden recycle bin folder for files recycled from that drive
- Recycle Bin folder structure is different on FAT and on NTFS drives

Recycle Bin on NTFS drives



SID Named Folder

$IYB6LR4.txt

$IAML6MK.mp4

$RYB6LR4.txt

$RAML6MK.mp4

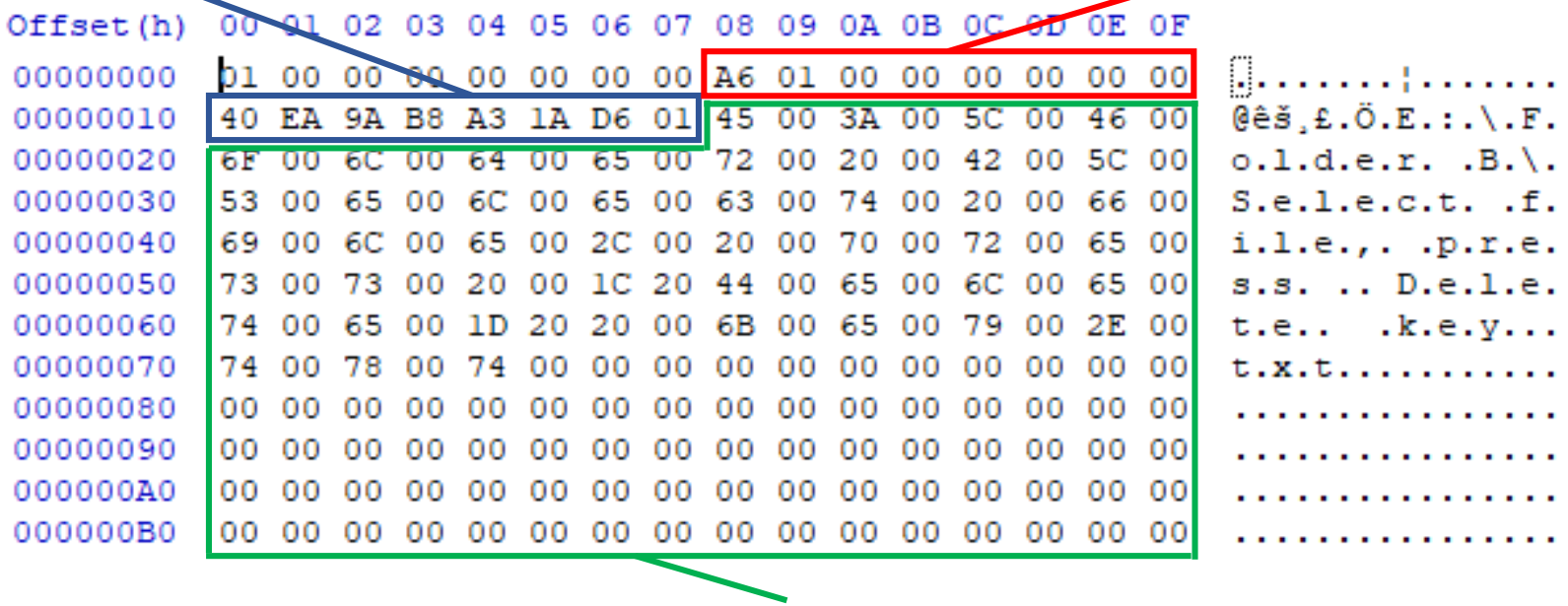
$I…files

- Have fixed size of 544 bytes
- Each $I… file contains info about the corresponding $R… file:
  - Size
  - Date and time of recycling
  - Original name and location

$IYB6LR4.txt

Dare & time of recycling
(Windows 64-bit timestamp)

Size of $R… file in bytes



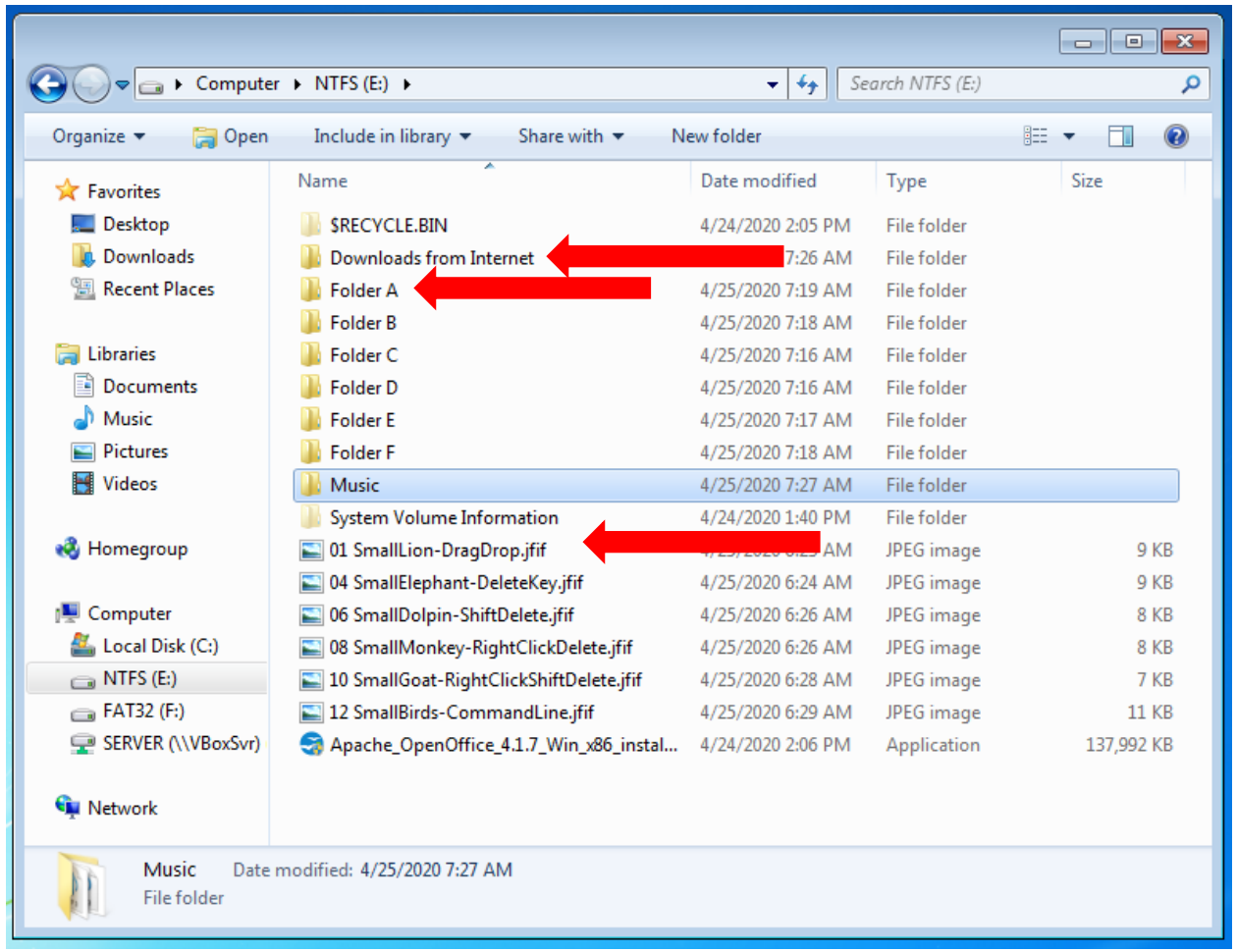
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	01	00	00	00	00	00	00	00	A6	01	00	00	00	00	00	00	..... ¦ .....
00000010	40	EA	9A	B8	A3	1A	D6	01	45	00	3A	00	5C	00	46	00	@êš¸£.Ö.E.:.\.F.
00000020	6F	00	6C	00	64	00	65	00	72	00	20	00	42	00	5C	00	o.l.d.e.r. .B.\.
00000030	53	00	65	00	6C	00	65	00	63	00	74	00	20	00	66	00	S.e.l.e.c.t. .f.
00000040	69	00	6C	00	65	00	2C	00	20	00	70	00	72	00	65	00	i.l.e.,. .p.r.e.
00000050	73	00	73	00	20	00	1C	20	44	00	65	00	6C	00	65	00	s.s. .. D.e.l.e.
00000060	74	00	65	00	1D	20	20	00	6B	00	65	00	79	00	2E	00	t.e.. .k.e.y...
00000070	74	00	78	00	74	00	00	00	00	00	00	00	00	00	00	00	t.x.t.....
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Original name and location of $R… file in Unicode

Practical Exercises

https://www.forensor.com/ramadhan1

Drag and drop file into Recycle Bin



Downloads from Internet

y2mate.com - KARTONYONO MEDOT JANJI – DENNY CAKNAN (Ipank Yuniar & Ulfah Betrianingsih Cover & Lirik)_K7REkdv7d7Y_720p.mp4

Folder A

02 BigLion-DragDrop.jpg

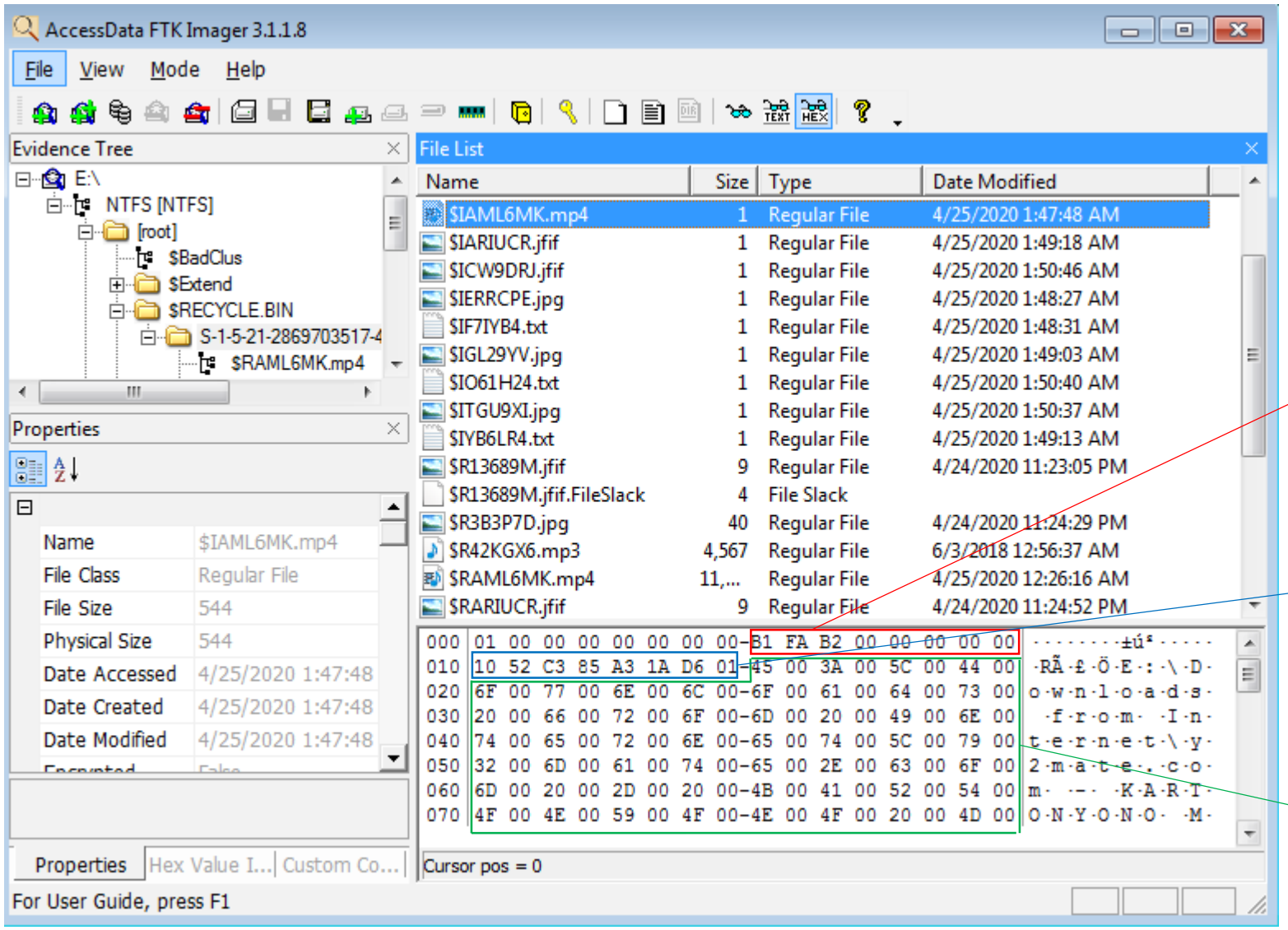
Drag and drop file into Recycle Bin.txt

Root Drive NTFS

01 SmallLion-DragDrop.jfif

Forensics Analysis of a File

y2mate.com - KARTONYONO.mp4



Name : $IAML6MK.mp4
File Size : 544 bytes
Physical Size : 544 bytes
Date Accessed : 4/25/2020 1:47:48 AM
Date Created : 4/25/2020 1:47:48 AM
Date Modified : 4/25/2020 1:47:48 AM

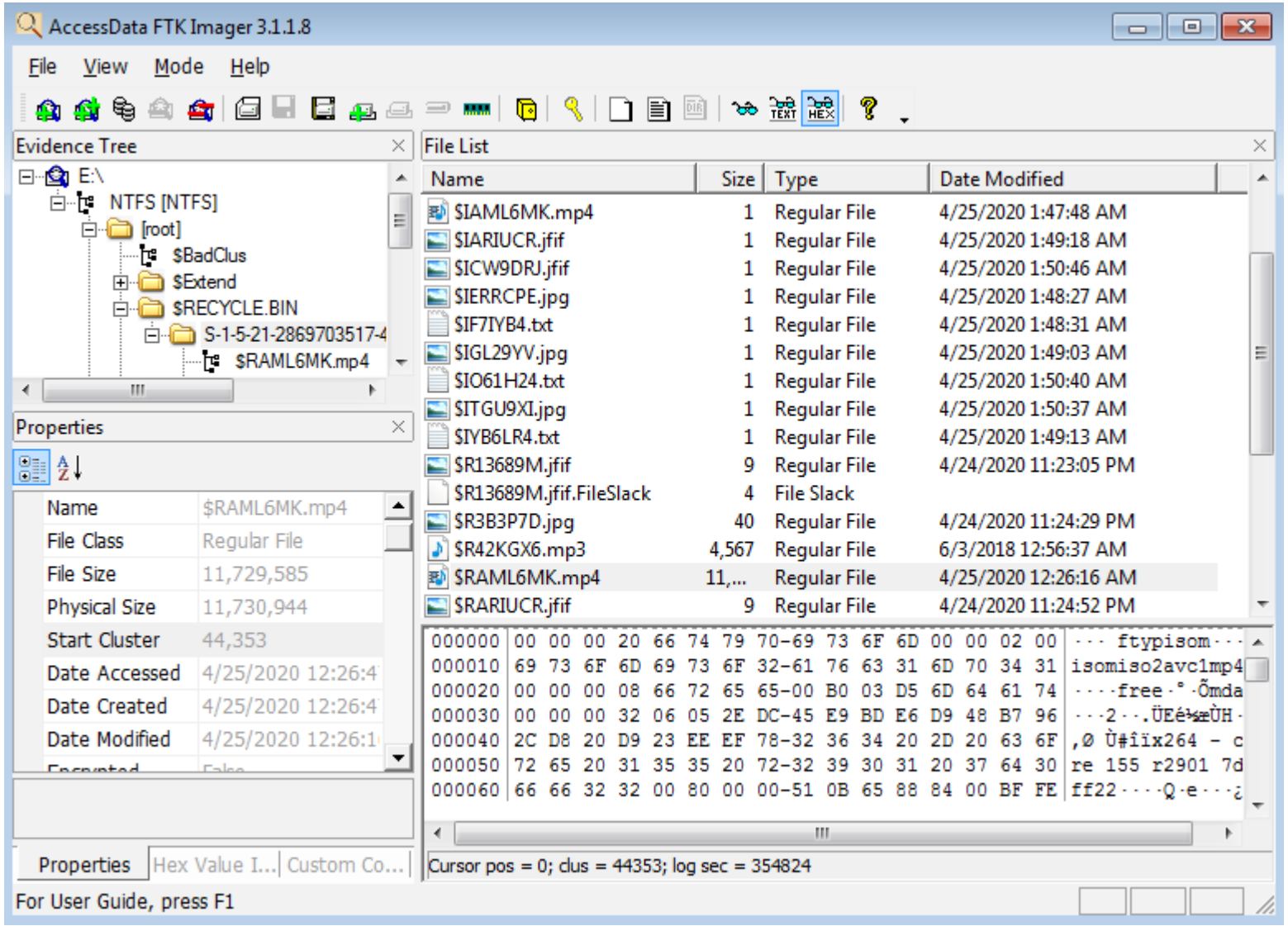
Size of $IAML6MK.mp4 file in bytes
32-bit LE Value B1FAB20000000000
00 B2 FA B1 = 11,729,585 bytes

Date & Time of Recycling
Decode Hex Value 1052C385A31AD601
Sat, 25 April 2020 01:47:48 UTC

Convert Hex Value to Unicode
E:\Downloads from Internet\y2mate.com – KARTONYONO MEDOT JANJI - DENNY CAKNAN (Ipank Yuniar & Ulfah Betrianingsih Cover & Lirik)_K7REkdv7d7Y_720p.mp4

Forensics Analysis of a File

y2mate.com - KARTONYONO.mp4

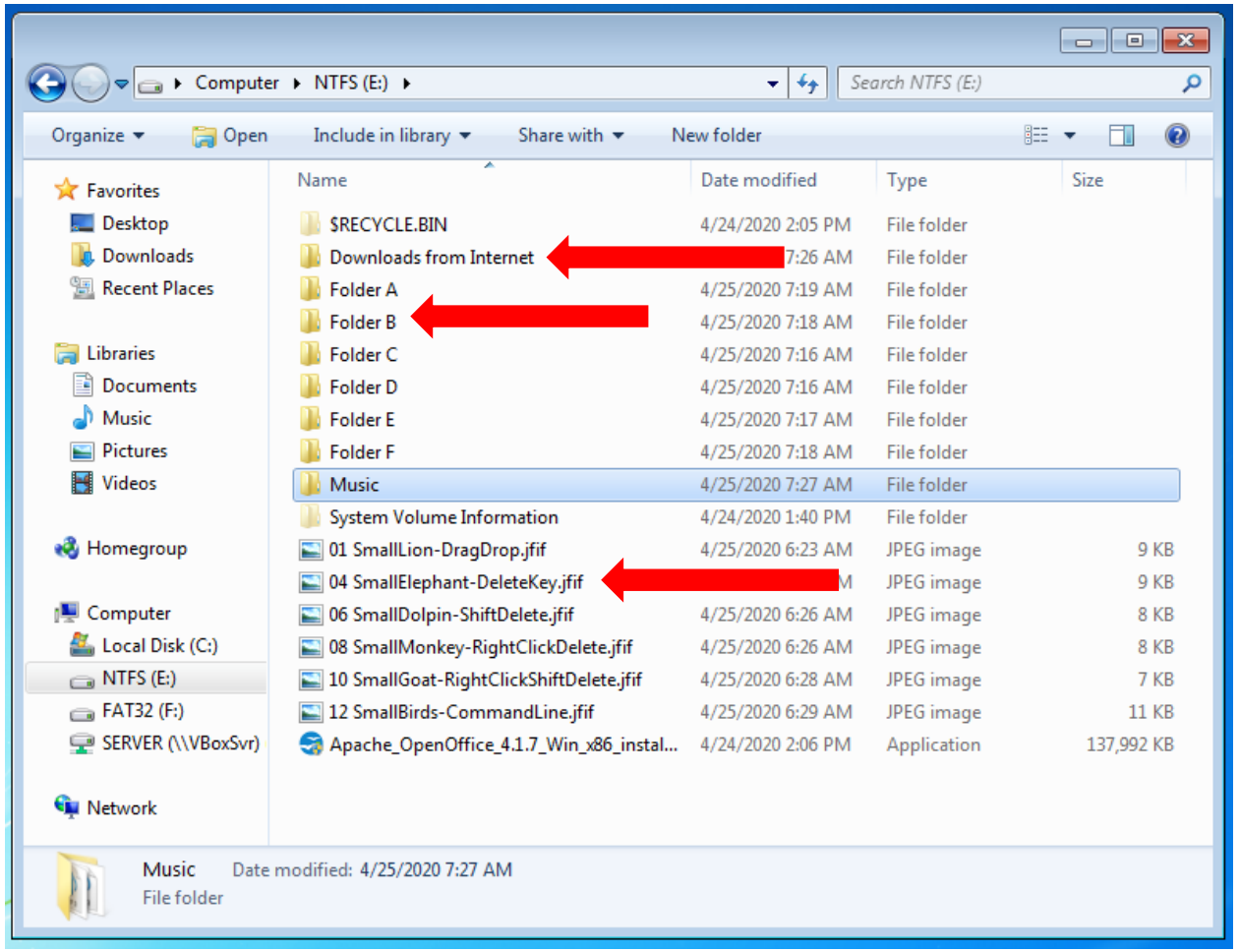


Name : $RAML6MK.mp4
File Size : 11,729,585 bytes
Physical Size : 11,730,944 bytes
Date Accessed : 4/25/2020 12:26:47 AM
Date Created : 4/25/2020 12:26:47 AM
Date Modified : 4/25/2020 12:26:16 AM

Original name and Location :
E:\Downloads from Internet\y2mate.com – KARTONYONO MEDOT JANJI - DENNY CAKNAN (Ipank Yuniar & Ulfah Betrianingsih Cover & Lirik)_K7REkdv7d7Y_720p.mp4
Size : 11,729,585 bytes
Date & Time of Recycling :
Sat, 25 April 2020 01:47:48 UTC
Deleted by Owner SID :
S-1-5-21-2869703517-4213650454-673425579-1001 (forensor)

```
C:\Windows\system32>wmic useraccount get name,sid
Name           SID
Administrator  S-1-5-21-2869703517-4213650454-673425579-500
forensor       S-1-5-21-2869703517-4213650454-673425579-1001
Guest          S-1-5-21-2869703517-4213650454-673425579-501
HomeGroupUser$ S-1-5-21-2869703517-4213650454-673425579-1002
```

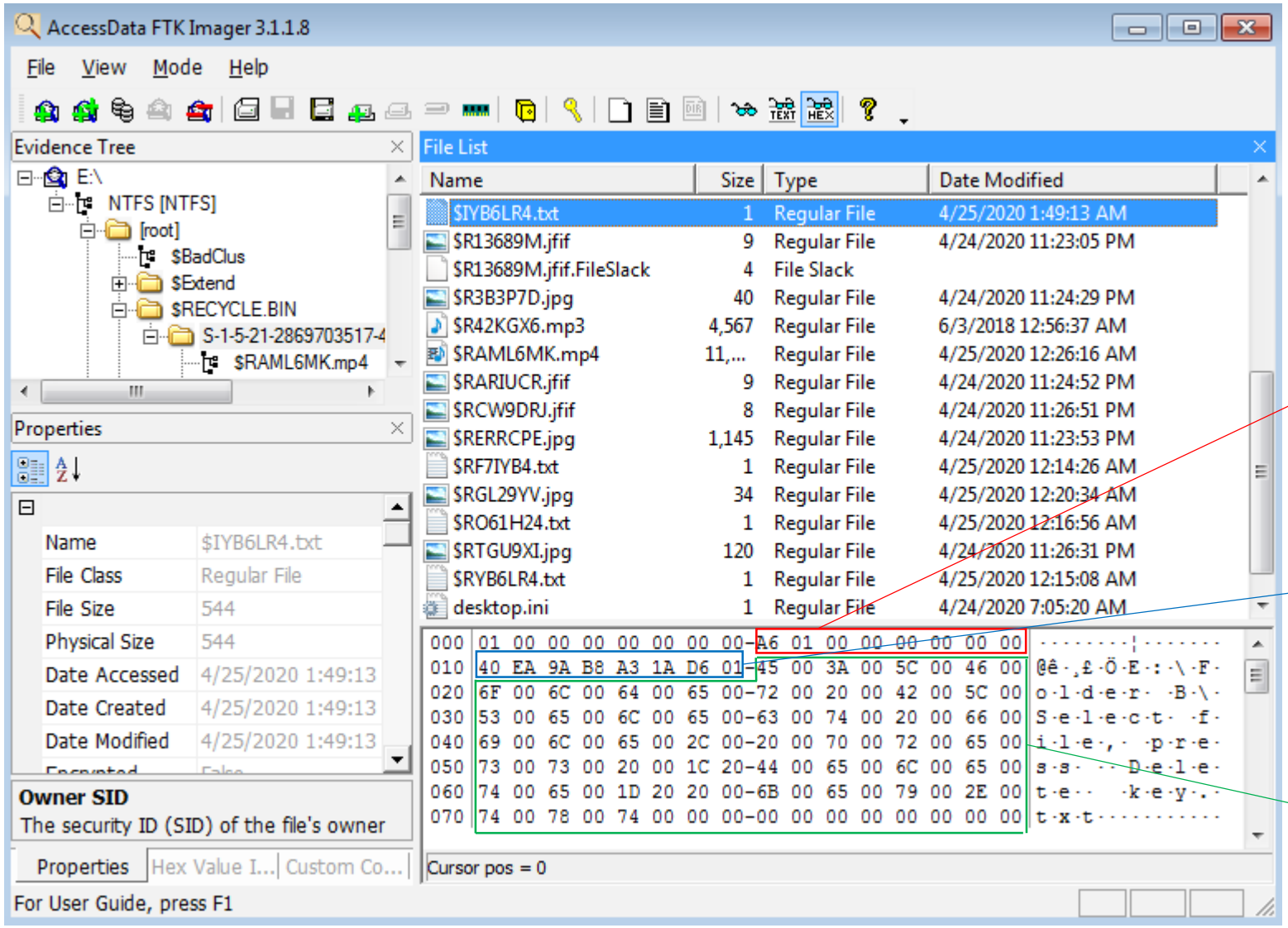
Select file, press “Delete” key



Download from Internet
1402558_1.jpg
Folder B
03 BigElephant-DeleteKey.jpg
Select file, press “Delete” key.txt
Root Drive NTFS
04 SmallElephant-DeleteKey.jfif

Forensics Analysis of a File

Select file, press "Delete" key.txt



Name : $IYB6LR4.txt
File Size : 544 bytes
Physical Size : 544 bytes
Date Accessed : 4/25/2020 1:49:13 AM
Date Created : 4/25/2020 1:49:13 AM
Date Modified : 4/25/2020 1:49:13 AM

Size of $RYB6LR4.txt file in bytes
16-bit LE Value A601000000000000
01 A6 = 422 bytes

Date & Time of Recycling
Decode Hex Value 40EA9AB8A31AD601
Sat, 25 April 2020 01:49:13 UTC

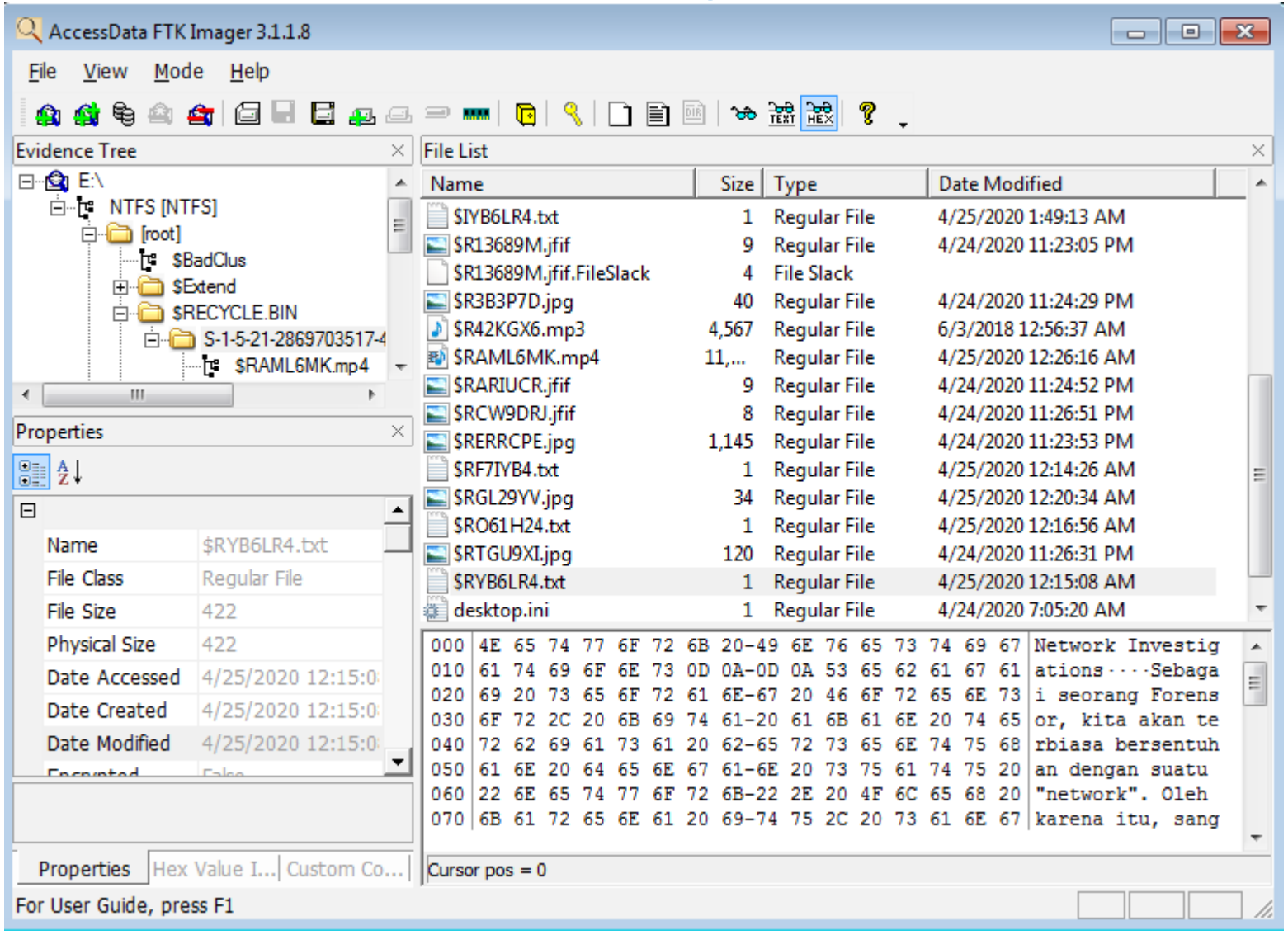
Convert Hex Value to Unicode

```
000 01 00 00 00 00 00 00 00-A6 01 00 00 00 00 00 00 ........¦........
010 40 EA 9A B8 A3 1A D6 01-45 00 3A 00 5C 00 46 00 @ê·¸£·Ö·E·:·\·F·
020 6F 00 6C 00 64 00 65 00-72 00 20 00 42 00 5C 00 o·l·d·e·r· ·B·\·
030 53 00 65 00 6C 00 65 00-63 00 74 00 20 00 66 00 S·e·l·e·c·t· ·f·
040 69 00 6C 00 65 00 2C 00-20 00 70 00 72 00 65 00 i·l·e·,· ·p·r·e·
050 73 00 73 00 20 00 1C 20-44 00 65 00 6C 00 65 00 s·s· ·· D·e·l·e·
060 74 00 65 00 1D 20 20 00-6B 00 65 00 79 00 2E 00 t·e·· ·k·e·y·.·
070 74 00 78 00 74 00 00 00-00 00 00 00 00 00 00 00 t·x·t···········
```

E:\Folder B\Select file, press "Delete" key.txt

Forensics Analysis of a File

Select file, press "Delete" key.txt

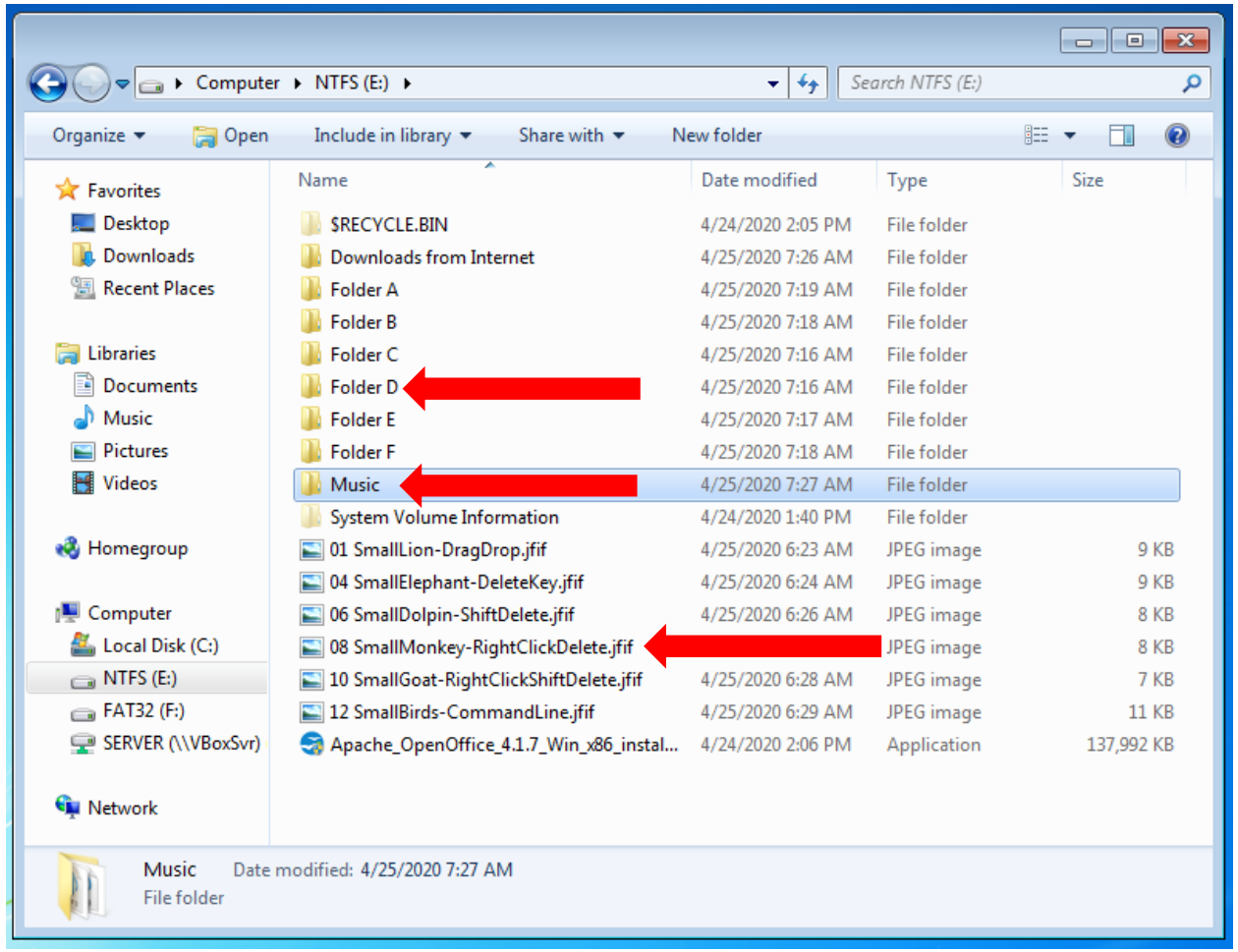


Name : $RYB6LR4.txt
File Size : 422 bytes
Physical Size : 422 bytes
Date Accessed : 4/25/2020 12:15:08 AM
Date Created : 4/25/2020 12:15:08 AM
Date Modified : 4/25/2020 12:15:08 AM

Original name :
Select file, press "Delete" key.txt
Path :
E:\Folder B\Select file, press "Delete" key.txt
Size : 422 bytes
Date & Time of Recycling :
Sat, 25 April 2020 01:49:13 UTC
Deleted by Owner SID :
S-1-5-21-2869703517-4213650454-673425579-1001 (forensor)

```
C:\Windows\system32>wmic useraccount get name,sid
Name           SID
Administrator  S-1-5-21-2869703517-4213650454-673425579-500
forensor       S-1-5-21-2869703517-4213650454-673425579-1001
Guest          S-1-5-21-2869703517-4213650454-673425579-501
HomeGroupUser$ S-1-5-21-2869703517-4213650454-673425579-1002
```

Select file, right-click, select “Delete” option



Music

y2mate.com - wali_band_ada_gajah_dibalik_batu_official_music_video_nagaswara_music_lcv-R5gVqCs.mp3

Folder D

07 BigMonkey-RightClickDelete.jpg

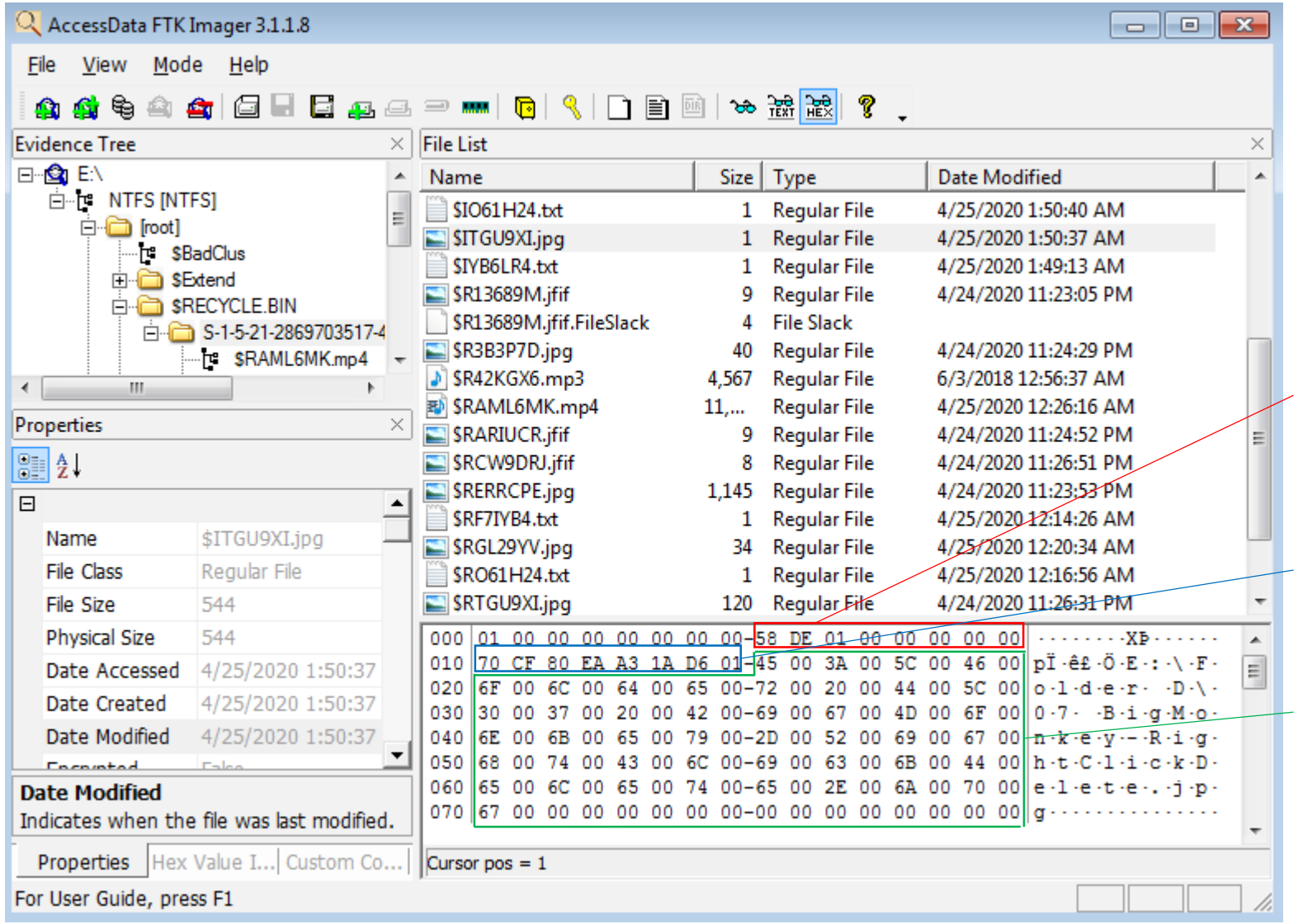
Select file, right-click, select “Delete” option.txt

Root Drive NTFS

08 SmallMonkey-RightClickDelete.jfif

Forensics Analysis of a File

07 BigMonkey-RightClickDelete.jpg



Name : $ITGU9XI.jpg
File Size : 544 bytes
Physical Size : 544 bytes
Date Accessed : 4/25/2020 1:50:37 AM
Date Created : 4/25/2020 1:50:37 AM
Date Modified : 4/25/2020 1:50:37 AM

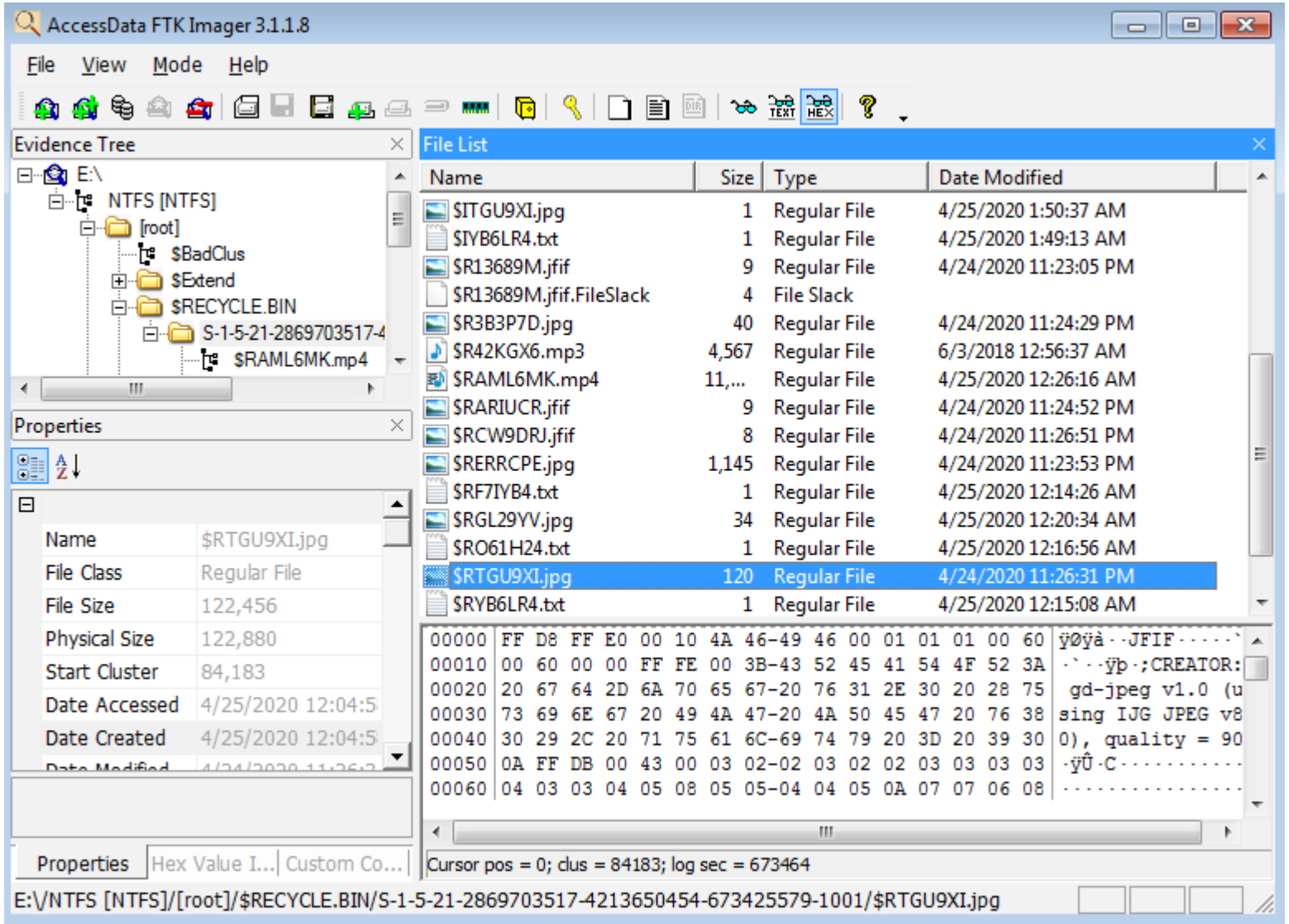
Size of $IAML6MK.mp4 file in bytes
32-bit LE Value 58DE010000000000
00 01 DE 58 = 122,456 bytes

Date & Time of Recycling
Decode Hex Value 70CF80EAA31AD601
Sat, 25 April 2020 01:50:37 UTC

Convert Hex Value to Unicode
E:\Folder D\07 BigMonkey-RightClickDelete.jpg

Forensics Analysis of a File

07 BigMonkey-RightClickDelete.jpg

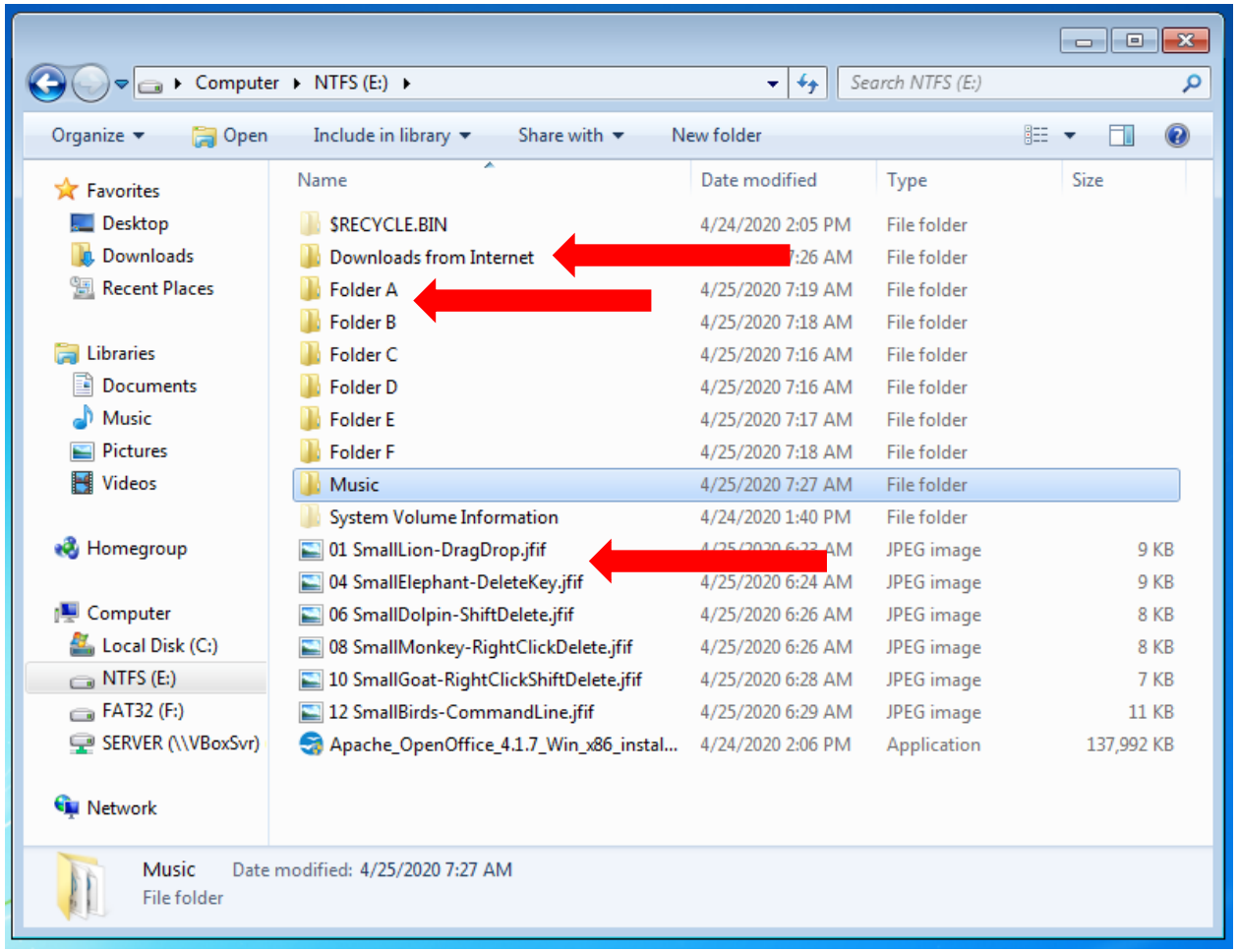


Name : $RTGU9XI.jpg
File Size : 122,456 bytes
Physical Size : 122,880 bytes
Date Accessed : 4/25/2020 12:04:58 AM
Date Created : 4/25/2020 12:04:58 AM
Date Modified : 4/24/2020 11:26:31 PM

Original name and Location :
E:\Folder D\07 BigMonkey-RightClickDelete.jpg
Size : 122,456 bytes
Date & Time of Recycling :
Sat, 25 April 2020 01:50:37 UTC
Deleted by Owner SID :
S-1-5-21-2869703517-4213650454-673425579-1001 (forensor)

```
C:\Windows\system32>wmic useraccount get name,sid
Name           SID
Administrator  S-1-5-21-2869703517-4213650454-673425579-500
forensor       S-1-5-21-2869703517-4213650454-673425579-1001
Guest          S-1-5-21-2869703517-4213650454-673425579-501
HomeGroupUser$ S-1-5-21-2869703517-4213650454-673425579-1002
```

Select file, press “Shift” and “Delete” keys



Download from Internet

y2mate.com - Maher Zain - Ramadan (English) _ Official Music Video_3G-t72JjRf0_720p.mp4

Folder C

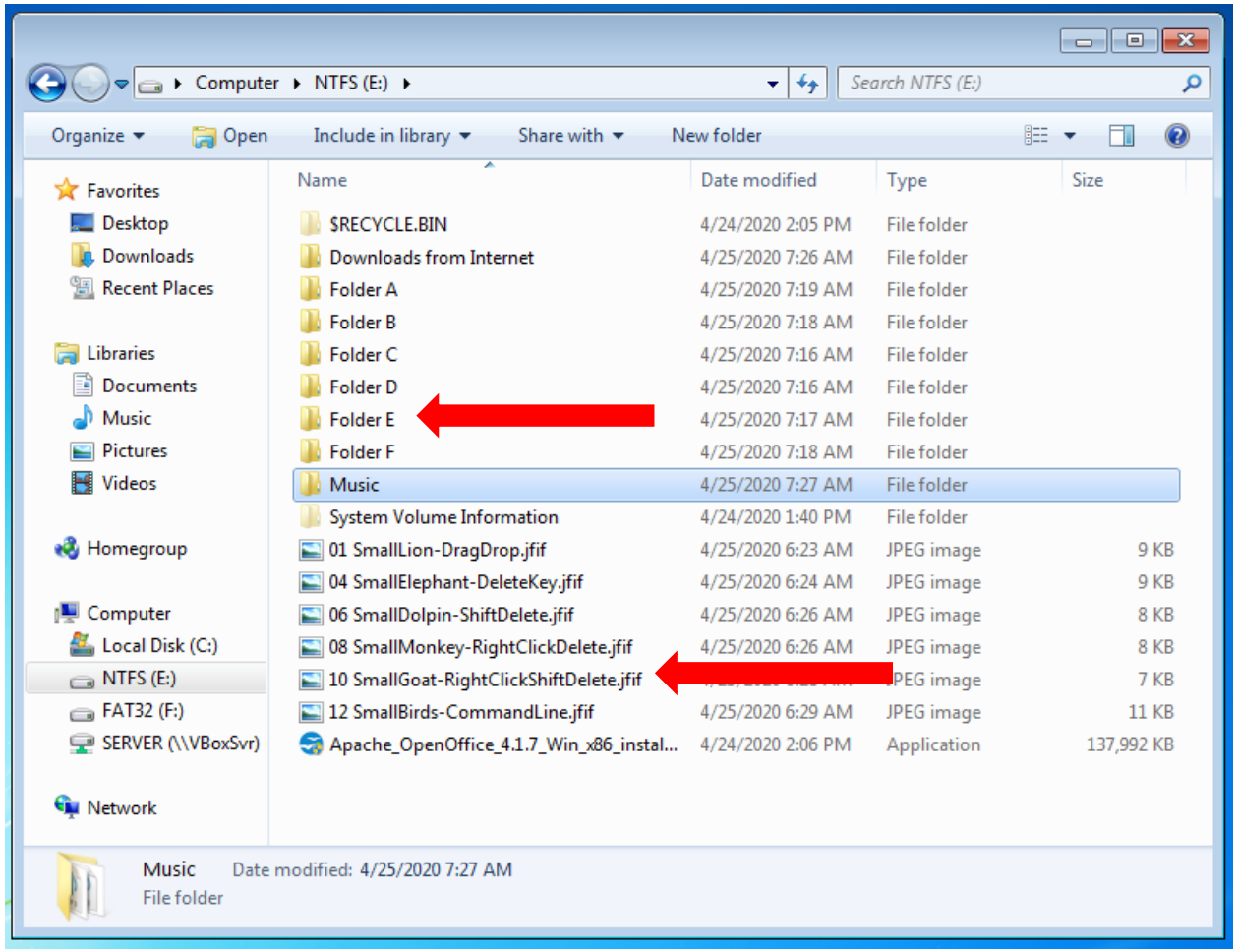
05 BigDolpin-ShiftDelete.jpg

Select file, press “Shift” and “Delete” keys.txt

Root Drive NTFS

06 SmallDolpin-ShiftDelete.jfif

Select file, right-click, press “Shift” key and select “Delete” option



Folder E

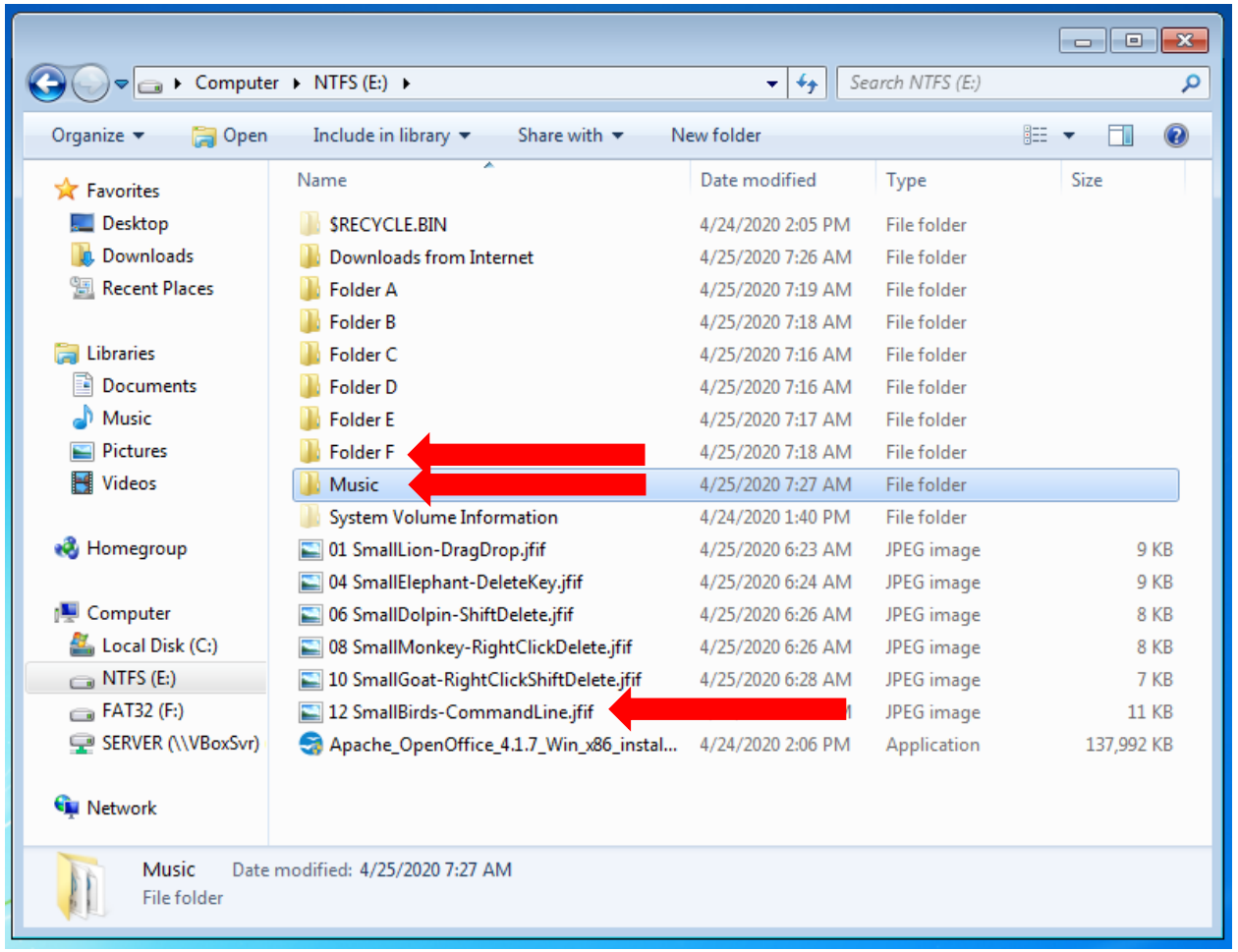
09 BigGoat-RightClickShiftDelete.jpg

Select file, right-click, press “Shift” key and select “Delete” option.txt

Root Drive NTFS

10 SmallGoat-RightClickShiftDelete.jfif

Delete file from command line



Music

y2mate.com - deen_assalam_cover_by_sabyan_1OMD_LSELAM.mp3

Folder F

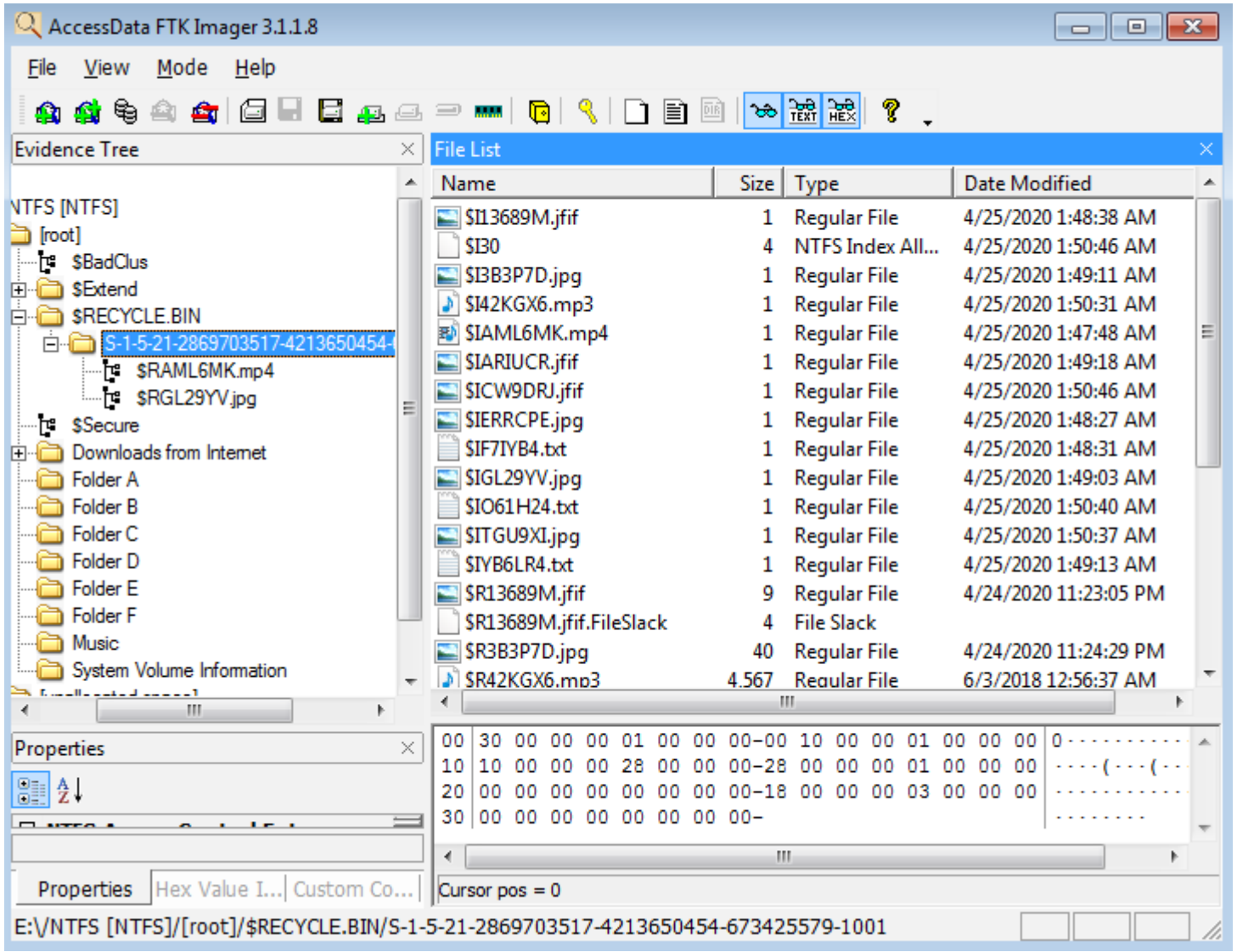
11 BigBirds-CommandLine.jpg

Delete file from command line.txt

Root Drive NTFS

12 SmallBirds-CommandLine.jfif

Forensics Analysis of 3 File Deletion Types

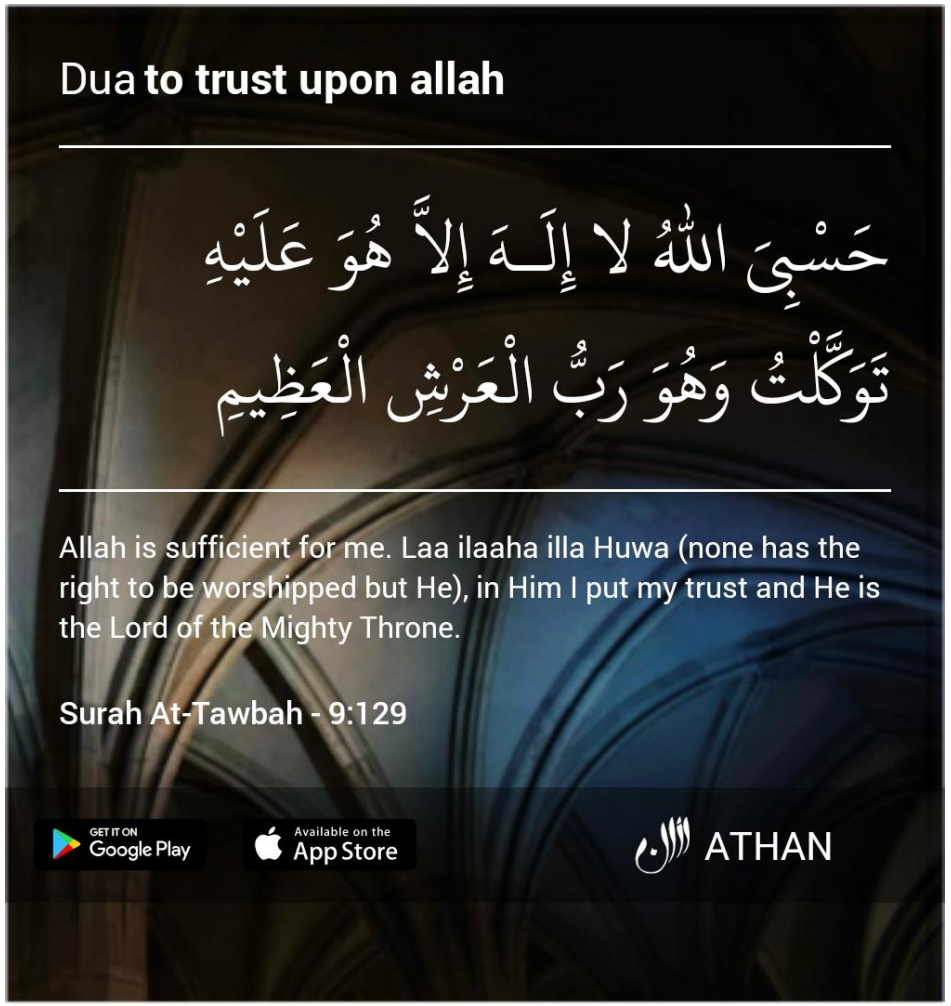


1. **All deleted files are moved permanently from the filesystem. No files found in the folder $Recycle.bin.**
2. **Area/space/cluster of all deleted files will be assigned as unallocated space/cluster. Then, all deleted files are still available as long as the space is not reused or the files are not overwritten.**
3. **How to recover from 3 type deletion type? Using DATA CARVING.**
4. **Watch the video to know how to manually carve the files -> https://www.forensor.com/ramadhan1**

Program Ramadhan Berbagi

Tools

- AccessData® FTK® Imager 3.1.1.8 from https://accessdata.com/
- DCode-v4.02a-build-4.02.0.9306 from https://www.digital-detective.co.uk/
- https://www.scadacore.com/tools/programming-calculators/online-hex-converter/
- https://www.binaryhexconverter.com/hex-to-ascii-text-converter



Follow the Facebook Page https://www.facebook.com/forensor for other sharing