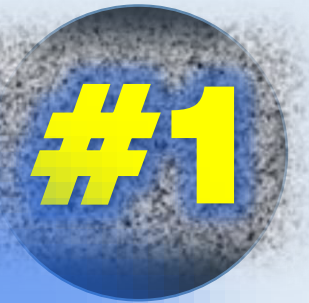


RAMADHAN BERBAGI #1

FORENSICS OF WINDOWS RECYCLE BIN



Izazi Mubarok





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

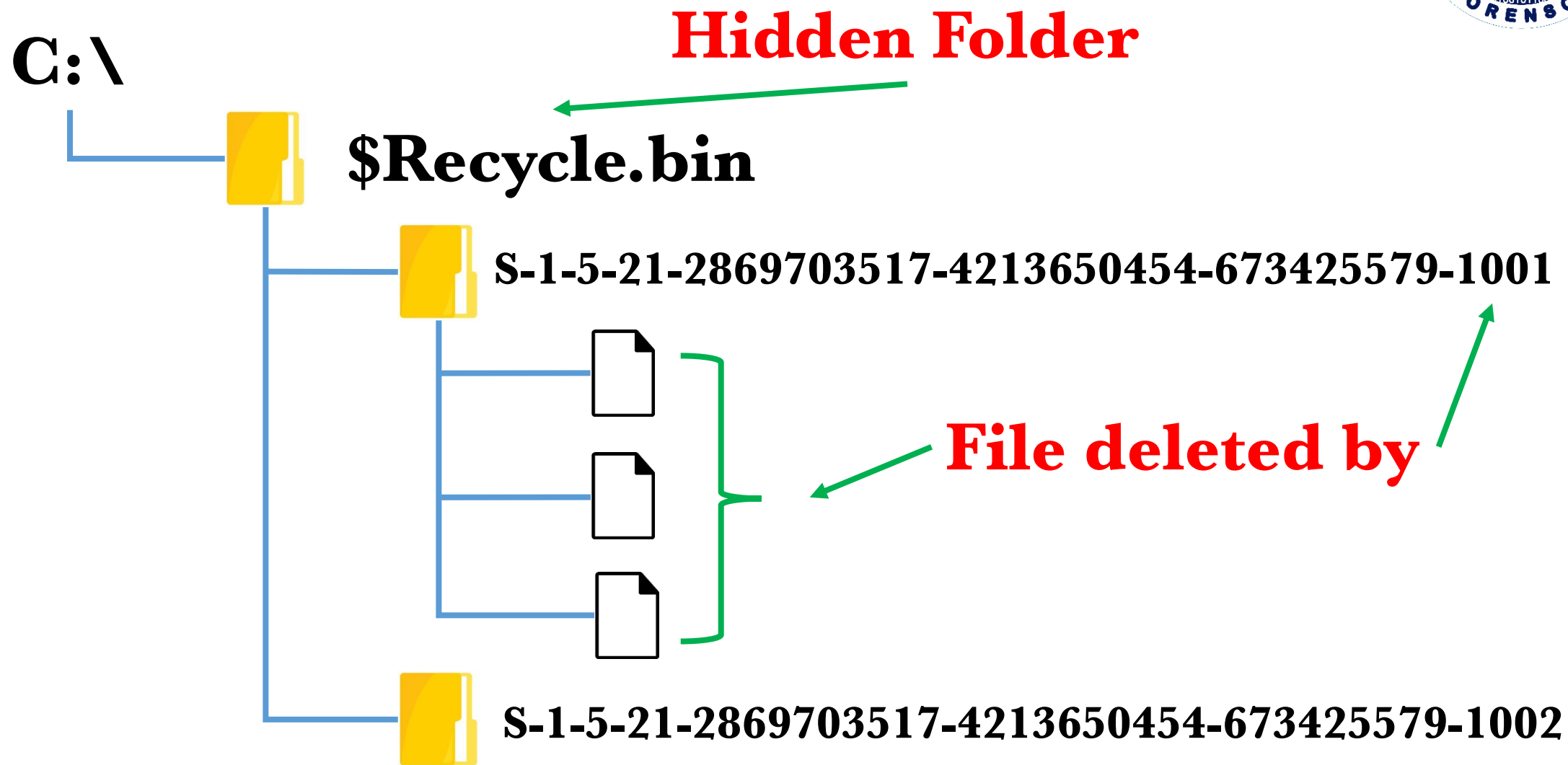


Folder Structure

- 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	@ès,£.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

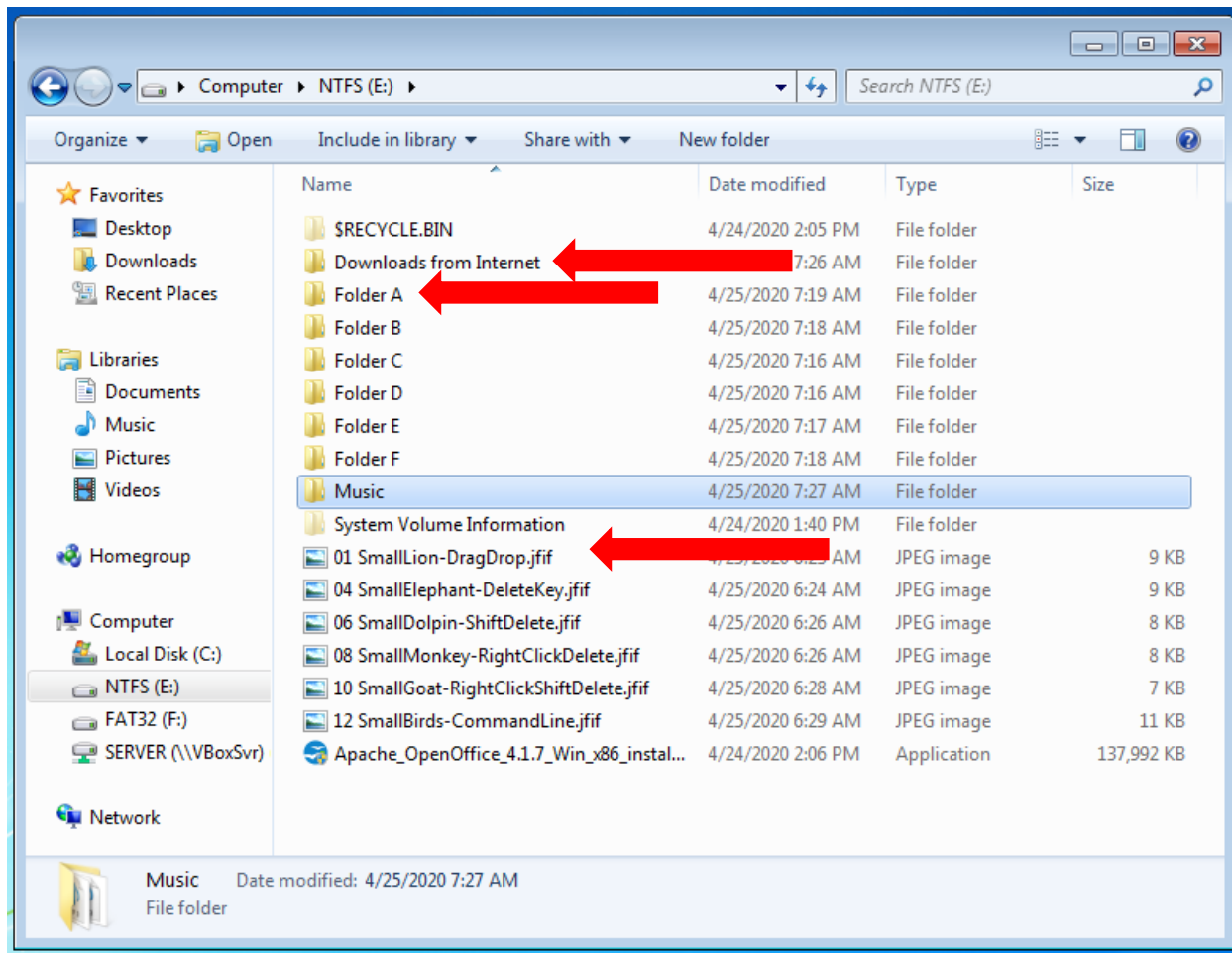
Original name and location of \$R... file in Unicode



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 : \$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
```

The screenshot shows the AccessData FTK Imager interface. The 'File List' pane displays a table of files in the current directory. The file '\$RAML6MK.mp4' is highlighted. The 'Properties' pane shows details for this file, including its size, physical size, and dates. The 'Hex Value' pane shows the raw data of the file, starting with 'ftypisom'.

Name	Size	Type	Date Modified
\$IAML6MK.mp4	1	Regular File	4/25/2020 1:47:48 AM
\$IARIUCR.jfif	1	Regular File	4/25/2020 1:49:18 AM
\$ICW9DRJ.jfif	1	Regular File	4/25/2020 1:50:46 AM
\$IERRCPE.jpg	1	Regular File	4/25/2020 1:48:27 AM
\$IF7IYB4.txt	1	Regular File	4/25/2020 1:48:31 AM
\$IGL29YV.jpg	1	Regular File	4/25/2020 1:49:03 AM
\$IO61H24.txt	1	Regular File	4/25/2020 1:50:40 AM
\$ITGU9XI.jpg	1	Regular File	4/25/2020 1:50:37 AM
\$IYB6LR4.txt	1	Regular File	4/25/2020 1:49:13 AM
\$R13689M.jfif	9	Regular File	4/24/2020 11:23:05 PM
\$R13689M.jfif.FileSlack	4	File Slack	
\$R3B3P7D.jpg	40	Regular File	4/24/2020 11:24:29 PM
\$R42KGX6.mp3	4,567	Regular File	6/3/2018 12:56:37 AM
\$RAML6MK.mp4	11,...	Regular File	4/25/2020 12:26:16 AM
\$RARIUCR.jfif	9	Regular File	4/24/2020 11:24:52 PM

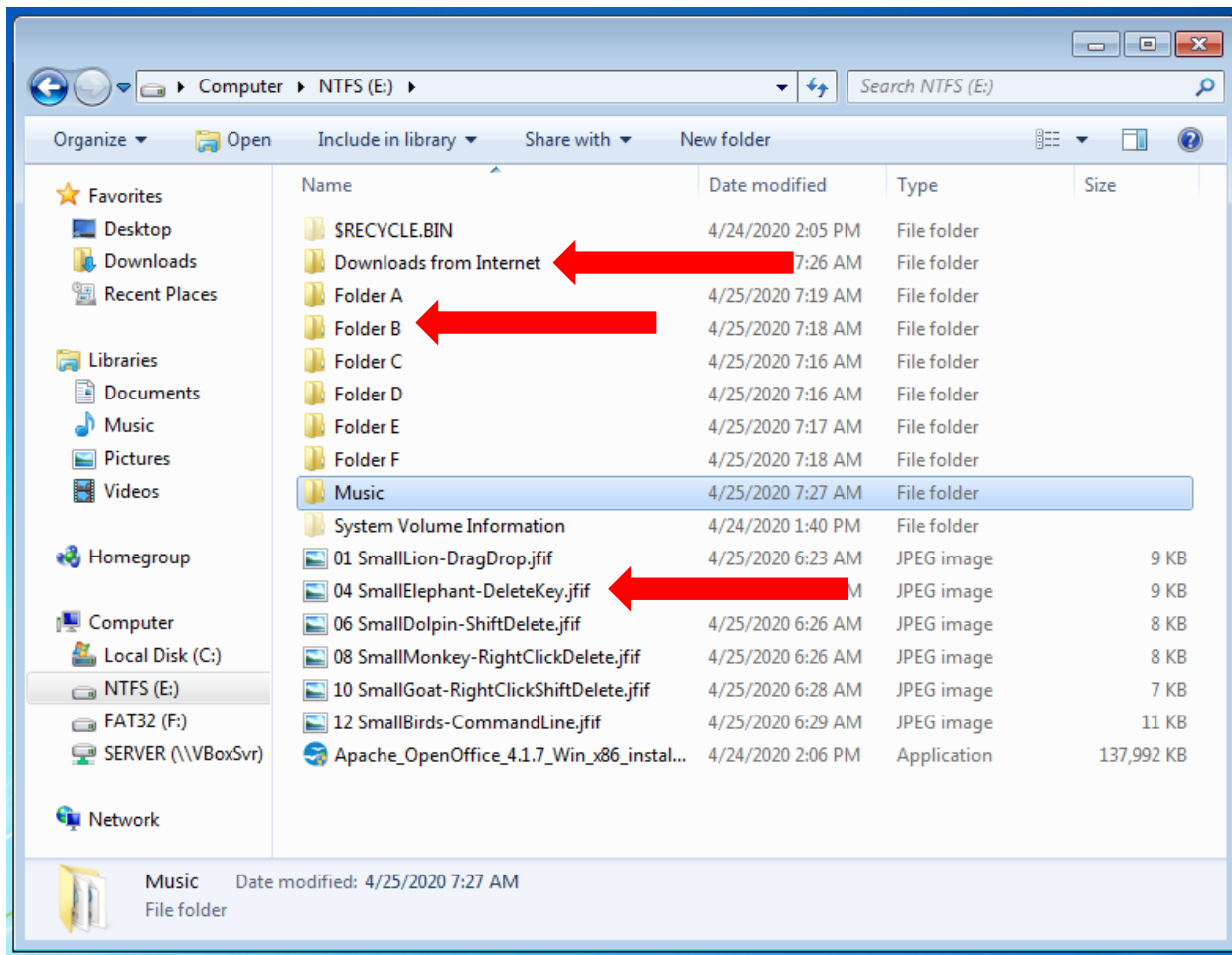
Properties for \$RAML6MK.mp4:

Name	\$RAML6MK.mp4
File Class	Regular File
File Size	11,729,585
Physical Size	11,730,944
Start Cluster	44,353
Date Accessed	4/25/2020 12:26:4
Date Created	4/25/2020 12:26:4
Date Modified	4/25/2020 12:26:1

Hex Value (ftypisom):

```
000000 00 00 00 20 66 74 79 70-69 73 6F 6D 00 00 02 00 ... ftypisom...
000010 69 73 6F 6D 69 73 6F 32-61 76 63 31 6D 70 34 31 isomiso2avclmp4
000020 00 00 00 08 66 72 65 65-00 B0 03 D5 6D 64 61 74 ... free- * -õmda
000030 00 00 00 32 06 05 2E DC-45 E9 BD E6 D9 48 B7 96 ... 2... ÜÉææÜH
000040 2C D8 20 D9 23 EE EF 78-32 36 34 20 2D 20 63 6F ,0 Ü#iix264 - c
000050 72 65 20 31 35 35 20 72-32 39 30 31 20 37 64 30 re 155 r2901 7d
000060 66 66 32 32 00 80 00 00-51 0B 65 88 84 00 BF FE ff22-...Q-e-...z
```


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 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

The screenshot shows the AccessData FTK Imager interface. The 'File List' pane displays a table of files in the root directory of a drive. The file '\$IYB6LR4.txt' is selected. The 'Properties' pane shows details for this file, including its size (544 bytes) and dates. The 'Hex' pane shows the raw data of the file, with a red box highlighting the hex value 'A6 01 00 00 00 00 00 00' and a green box highlighting the hex value '40 EA 9A B8 A3 1A D6 01'.

Name	Size	Type	Date Modified
\$IYB6LR4.txt	1	Regular File	4/25/2020 1:49:13 AM
SR13689M.jfif	9	Regular File	4/24/2020 11:23:05 PM
SR13689M.jfif.FileSlack	4	File Slack	
SR3B3P7D.jpg	40	Regular File	4/24/2020 11:24:29 PM
SR42KGX6.mp3	4,567	Regular File	6/3/2018 12:56:37 AM
SRAML6MK.mp4	11,...	Regular File	4/25/2020 12:26:16 AM
SRARIUCR.jfif	9	Regular File	4/24/2020 11:24:52 PM
SRCW9DRJ.jfif	8	Regular File	4/24/2020 11:26:51 PM
SRERRCPE.jpg	1,145	Regular File	4/24/2020 11:23:53 PM
SRF7IYB4.txt	1	Regular File	4/25/2020 12:14:26 AM
SRGL29YV.jpg	34	Regular File	4/25/2020 12:20:34 AM
SRO61H24.txt	1	Regular File	4/25/2020 12:16:56 AM
SRTGU9XI.jpg	120	Regular File	4/24/2020 11:26:31 PM
SRYB6LR4.txt	1	Regular File	4/25/2020 12:15:08 AM
desktop.ini	1	Regular File	4/24/2020 7:05:20 AM

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
```

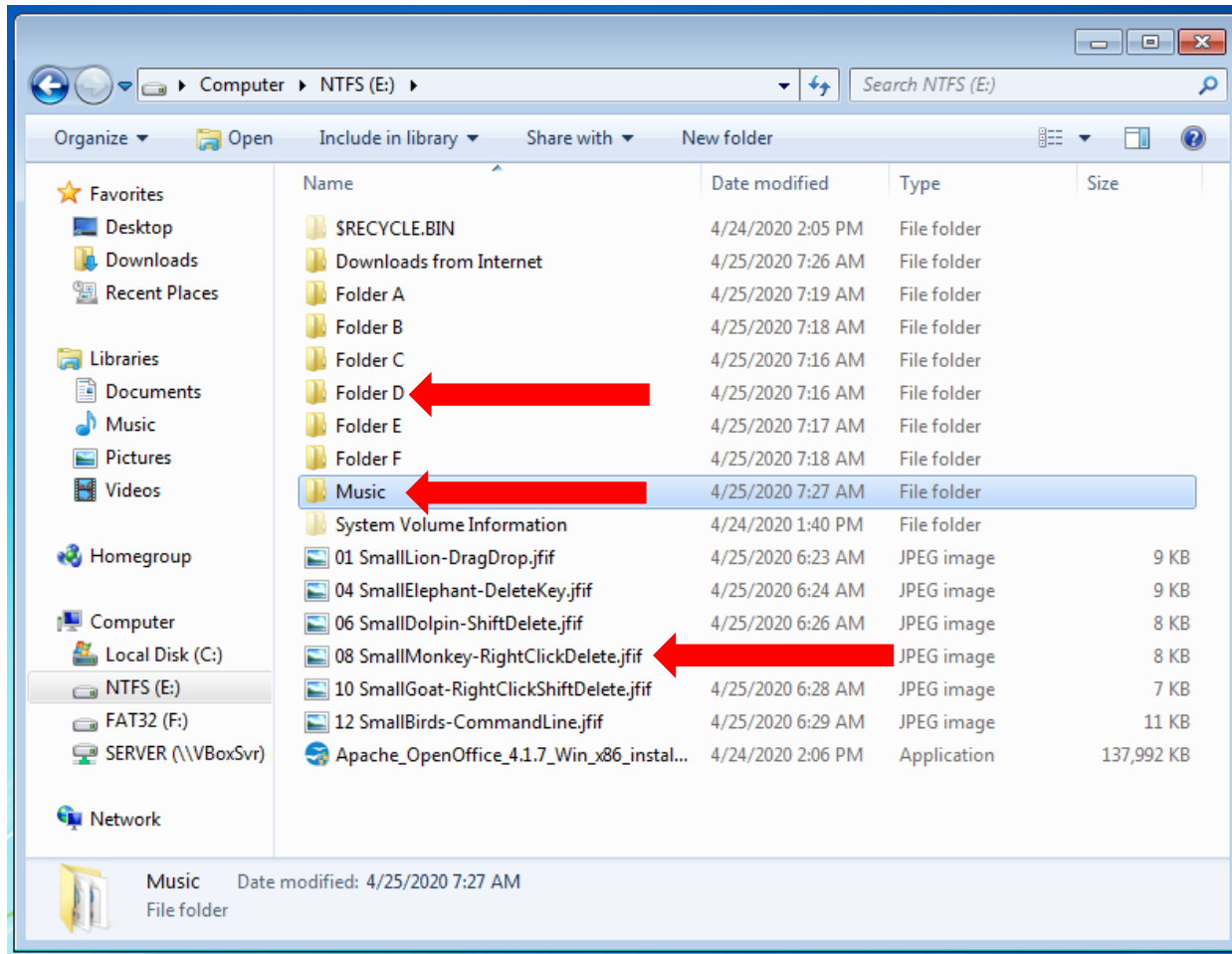
The screenshot shows the AccessData FTK Imager interface. The 'File List' pane displays a table of files in the current directory. The file '\$RYB6LR4.txt' is selected. The 'Properties' pane shows details for this file, including its name, class, size, physical size, and timestamps. The 'Hex Value I...' pane shows the raw data of the file, which appears to be a text file containing a network investigation report snippet.

Name	Size	Type	Date Modified
\$IYB6LR4.txt	1	Regular File	4/25/2020 1:49:13 AM
SR13689M.jfif	9	Regular File	4/24/2020 11:23:05 PM
SR13689M.jfif.FileSlack	4	File Slack	
SR3B3P7D.jpg	40	Regular File	4/24/2020 11:24:29 PM
SR42KGX6.mp3	4,567	Regular File	6/3/2018 12:56:37 AM
SRAML6MK.mp4	11,...	Regular File	4/25/2020 12:26:16 AM
SRARIUCR.jfif	9	Regular File	4/24/2020 11:24:52 PM
SRCW9DRJ.jfif	8	Regular File	4/24/2020 11:26:51 PM
SRERRCPE.jpg	1,145	Regular File	4/24/2020 11:23:53 PM
SRF7IYB4.txt	1	Regular File	4/25/2020 12:14:26 AM
SRGL29YV.jpg	34	Regular File	4/25/2020 12:20:34 AM
SRO61H24.txt	1	Regular File	4/25/2020 12:16:56 AM
SRTGU9XI.jpg	120	Regular File	4/24/2020 11:26:31 PM
SRYB6LR4.txt	1	Regular File	4/25/2020 12:15:08 AM
desktop.ini	1	Regular File	4/24/2020 7:05:20 AM

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


```
000 4E 65 74 77 6F 72 6B 20-49 6E 76 65 73 74 69 67 Network Investig
010 61 74 69 6F 6E 73 0D 0A-0D 0A 53 65 62 61 67 61 ations...Sebaga
020 69 20 73 65 6F 72 61 6E-67 20 46 6F 72 65 6E 73 i seorang Forens
030 6F 72 2C 20 6B 69 74 61-20 61 6B 61 6E 20 74 65 or, kita akan te
040 72 62 69 61 73 61 20 62-65 72 73 65 6E 74 75 68 rbiasa bersentuh
050 61 6E 20 64 65 6E 67 61-6E 20 73 75 61 74 75 20 an dengan suatu
060 22 6E 65 74 77 6F 72 6B-22 2E 20 4F 6C 65 68 20 "network". Oleh
070 6B 61 72 65 6E 61 20 69-74 75 2C 20 73 61 6E 67 karena itu, sang
```

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

The screenshot shows the AccessData FTK Imager interface. The 'File List' pane displays a table of files:

Name	Size	Type	Date Modified
\$IO61H24.txt	1	Regular File	4/25/2020 1:50:40 AM
\$ITGU9XI.jpg	1	Regular File	4/25/2020 1:50:37 AM
\$IYB6LR4.txt	1	Regular File	4/25/2020 1:49:13 AM
\$R13689M.jfif	9	Regular File	4/24/2020 11:23:05 PM
\$R13689M.jfif.FileSlack	4	File Slack	
\$R3B3P7D.jpg	40	Regular File	4/24/2020 11:24:29 PM
\$R42KGX6.mp3	4,567	Regular File	6/3/2018 12:56:37 AM
\$RAML6MK.mp4	11,...	Regular File	4/25/2020 12:26:16 AM
\$RARIUCR.jfif	9	Regular File	4/24/2020 11:24:52 PM
\$RCW9DRJ.jfif	8	Regular File	4/24/2020 11:26:51 PM
\$RERRCPE.jpg	1,145	Regular File	4/24/2020 11:23:53 PM
\$RF7IYB4.txt	1	Regular File	4/25/2020 12:14:26 AM
\$RGL29YV.jpg	34	Regular File	4/25/2020 12:20:34 AM
\$RO61H24.txt	1	Regular File	4/25/2020 12:16:56 AM
\$RTGU9XI.jpg	120	Regular File	4/24/2020 11:26:31 PM

The 'Properties' pane shows details for \$ITGU9XI.jpg:

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

The hex view shows the following data:

```
000 01 00 00 00 00 00 00 00 58 DE 01 00 00 00 00 00 .....Xp.....
010 70 CF 80 EA A3 1A D6 01 45 00 3A 00 5C 00 46 00 pï·ê£·Ö·E·:·\·F·
020 6F 00 6C 00 64 00 65 00-72 00 20 00 44 00 5C 00 o·l·d·e·r· ·D·\·
030 30 00 37 00 20 00 42 00-69 00 67 00 4D 00 6F 00 0·7· ·B·i·g·M·o·
040 6E 00 6B 00 65 00 79 00-2D 00 52 00 69 00 67 00 n·k·e·y· ·R·i·g·
050 68 00 74 00 43 00 6C 00-69 00 63 00 6B 00 44 00 h·t·C·l·i·c·k·D·
060 65 00 6C 00 65 00 74 00-65 00 2E 00 6A 00 70 00 e·l·e·t·e· ·j·p·
070 67 00 00 00 00 00 00 00-00 00 00 00 00 00 00 g·.....
```

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
```

The screenshot shows the AccessData FTK Imager interface. The 'Evidence Tree' on the left shows the file path: E:\NTFS [NTFS] [root] \$RECYCLE.BIN S-1-5-21-2869703517-4213650454-673425579-1001 \$RTGU9XI.jpg. The 'File List' table is as follows:

Name	Size	Type	Date Modified
SITGU9XI.jpg	1	Regular File	4/25/2020 1:50:37 AM
SIYB6LR4.txt	1	Regular File	4/25/2020 1:49:13 AM
SR13689M.jfif	9	Regular File	4/24/2020 11:23:05 PM
SR13689M.jfif.FileSlack	4	File Slack	
SR3B3P7D.jpg	40	Regular File	4/24/2020 11:24:29 PM
SR42KGX6.mp3	4,567	Regular File	6/3/2018 12:56:37 AM
SRAML6MK.mp4	11,...	Regular File	4/25/2020 12:26:16 AM
SRARIUCR.jfif	9	Regular File	4/24/2020 11:24:52 PM
SRCW9DRJ.jfif	8	Regular File	4/24/2020 11:26:51 PM
SRERRCPE.jpg	1,145	Regular File	4/24/2020 11:23:53 PM
SRF7IYB4.txt	1	Regular File	4/25/2020 12:14:26 AM
SRGL29YV.jpg	34	Regular File	4/25/2020 12:20:34 AM
SRO61H24.txt	1	Regular File	4/25/2020 12:16:56 AM
\$RTGU9XI.jpg	120	Regular File	4/24/2020 11:26:31 PM
SRYB6LR4.txt	1	Regular File	4/25/2020 12:15:08 AM

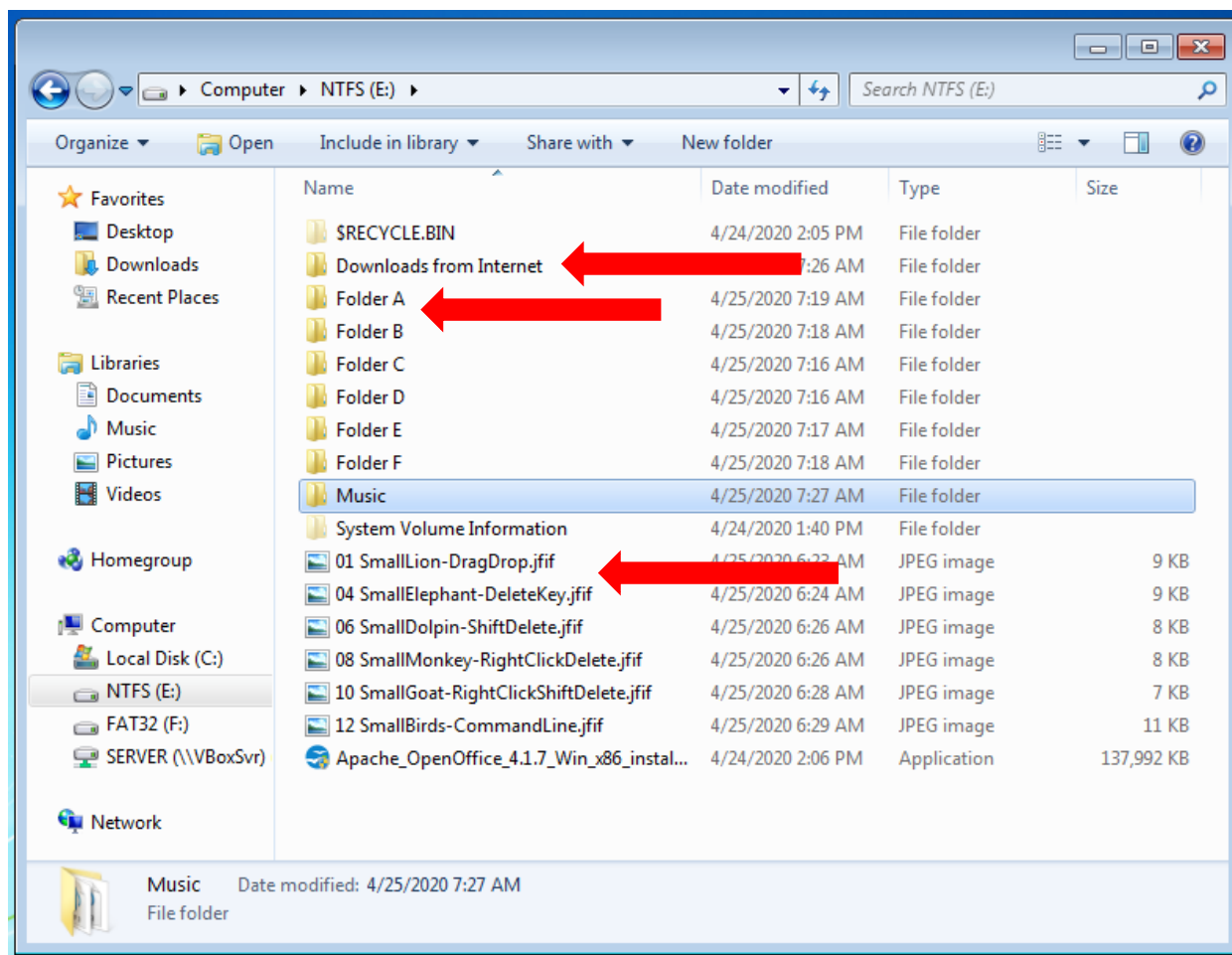
The 'Properties' window for \$RTGU9XI.jpg shows:

- Name: \$RTGU9XI.jpg
- File Class: Regular File
- File Size: 122,456
- Physical Size: 122,880
- Start Cluster: 84,183
- Date Accessed: 4/25/2020 12:04:5
- Date Created: 4/25/2020 12:04:5
- Date Modified: 4/24/2020 11:26:3

The hex view at the bottom shows the start of a JPEG file header: 000000 FF D8 FF E0 00 10 4A 46-49 46 00 01 01 01 00 60 yÿà··JFIF·...



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

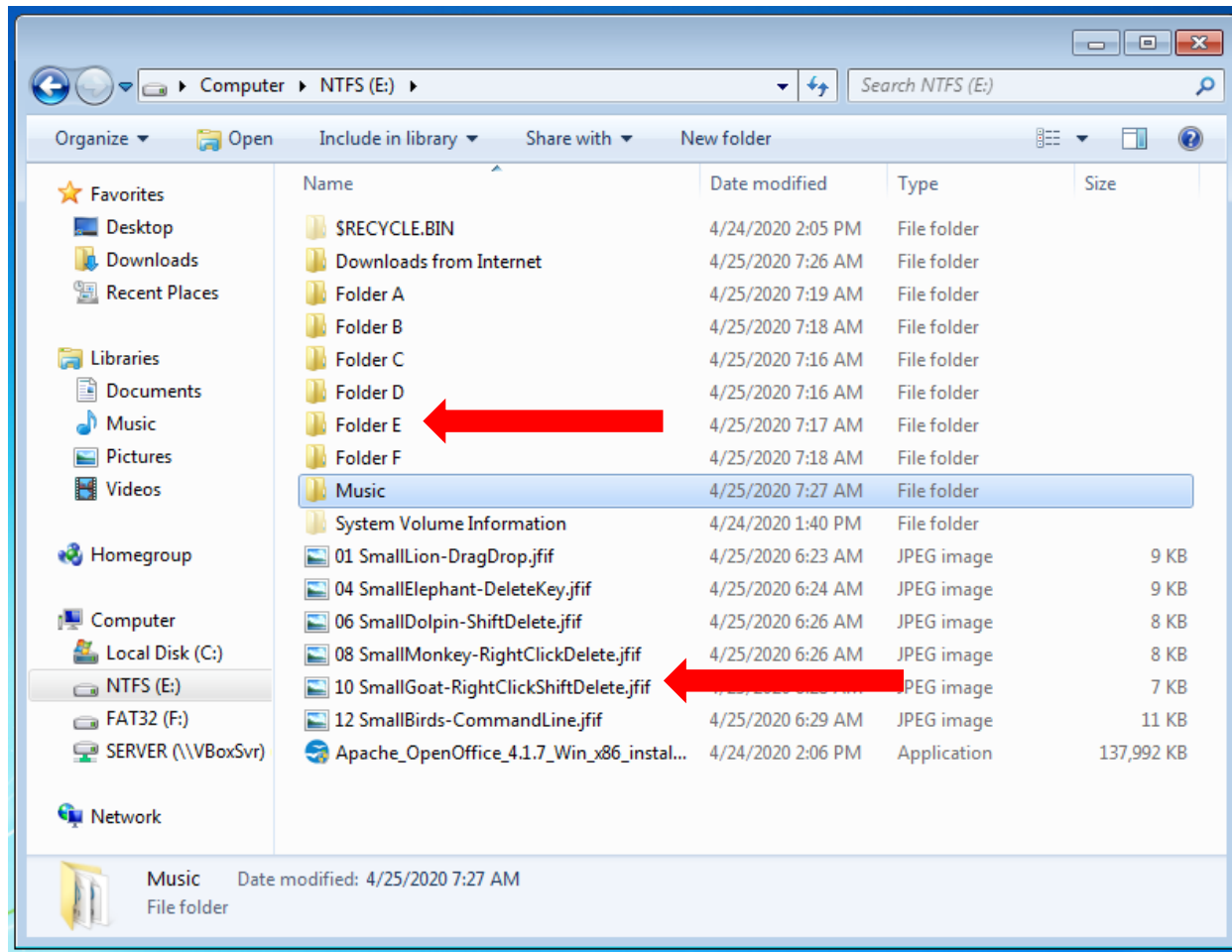
05 BigDolpin-ShiftDelete.jpg

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

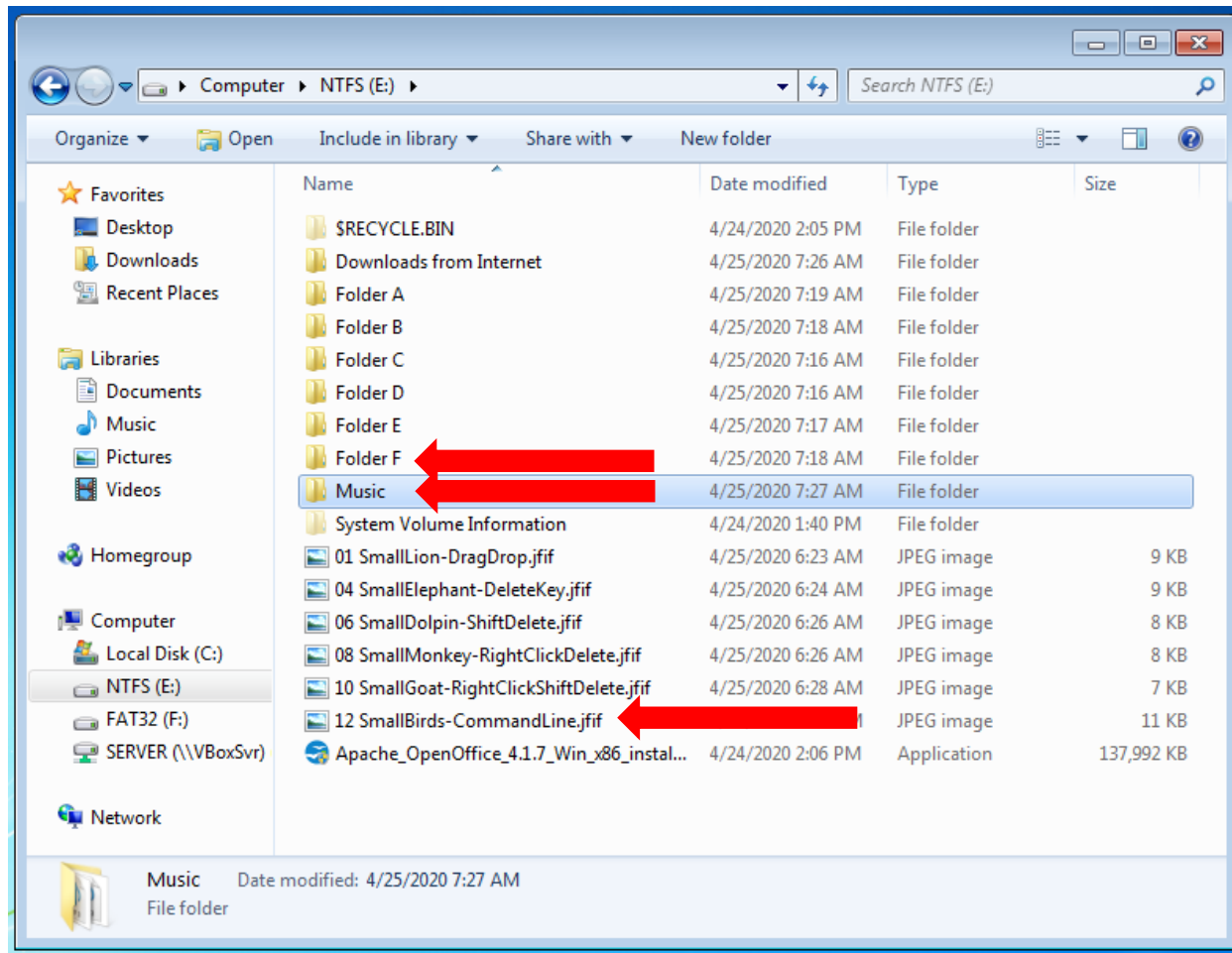
Select file, right-click, press “Shift” key and select “Delete” option.txt

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



Name	Size	Type	Date Modified
\$I13689M.jfif	1	Regular File	4/25/2020 1:48:38 AM
\$I30	4	NTFS Index All...	4/25/2020 1:50:46 AM
\$I3B3P7D.jpg	1	Regular File	4/25/2020 1:49:11 AM
\$I42KGX6.mp3	1	Regular File	4/25/2020 1:50:31 AM
\$IAML6MK.mp4	1	Regular File	4/25/2020 1:47:48 AM
\$IARIUCR.jfif	1	Regular File	4/25/2020 1:49:18 AM
\$ICW9DRJ.jfif	1	Regular File	4/25/2020 1:50:46 AM
\$IERRCPE.jpg	1	Regular File	4/25/2020 1:48:27 AM
\$IF7YB4.txt	1	Regular File	4/25/2020 1:48:31 AM
\$IGL29YV.jpg	1	Regular File	4/25/2020 1:49:03 AM
\$IO61H24.txt	1	Regular File	4/25/2020 1:50:40 AM
\$ITGU9XI.jpg	1	Regular File	4/25/2020 1:50:37 AM
\$IYB6LR4.txt	1	Regular File	4/25/2020 1:49:13 AM
\$R13689M.jfif	9	Regular File	4/24/2020 11:23:05 PM
\$R13689M.jfif.FileSlack	4	File Slack	
\$R3B3P7D.jpg	40	Regular File	4/24/2020 11:24:29 PM
\$R42KGX6.mp3	4.567	Regular File	6/3/2018 12:56:37 AM

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>

Dua to trust upon allah

حَسْبِيَ اللَّهُ لَا إِلَهَ إِلَّا هُوَ عَلَيْهِ
تَوَكَّلْتُ وَهُوَ رَبُّ الْعَرْشِ الْعَظِيمِ

Allah is sufficient for me. Laa ilaaha illa Huwa (none has the right to be worshipped but He), in Him I put my trust and He is the Lord of the Mighty Throne.

Surah At-Tawbah - 9:129

GET IT ON Google Play Available on the App Store

ATHAN

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