Features

SYNTRICATE

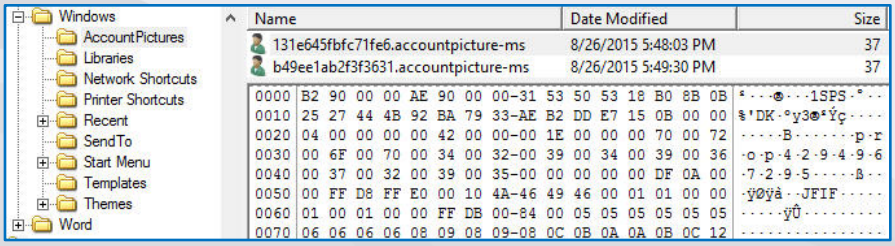
- Return of the Start Button
- Cortana
- Microsoft Edge / Project Spartan
- OneDrive
- OneNote
- EFS (changed)
- Defrag
- Recycle Bin
- Prefetch
- Thumbcache
- Registry Changes
- Metro Apps now called Windows Apps
  - Mail
  - Xbox App
  - Video / Photo Apps
  - Office Universal Apps

User Logon Icon

SYNTRICATE

- The user's logon thumbnail is a jpg graphic
- It has no extension and is a –ms file
- The user's logon thumbnail is stored at:

C:\Users\<username>\AppData\Roaming\Microsoft\Windows\AccountPictures

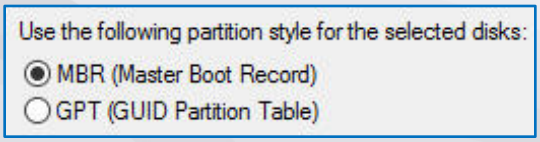


SYNTRICATE

Supported Partition Types

SYNTRICATE

- Partition Type Support
  - MBR
  - GPT
- Supports internal created VHDs
- Internal Mounting of ISO files



SYNTRICATE

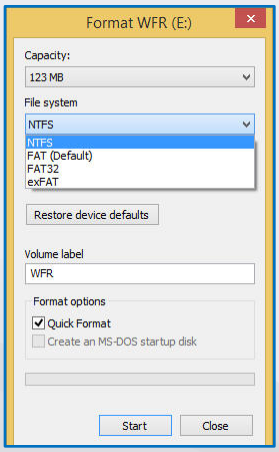
NTFS Version

SYNTRICATE

- Windows 10 continues using the NTFS 3.1 version in play since Windows XP

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>fsutil fsinfo ntfsinfo c:
NTFS Volume Serial Number :       0x385894765894349a
NTFS Version   :                  3.1
LFS Version    :                  2.0
Number Sectors :                  0x000000001defc7ff
Total Clusters :                  0x0000000003bdf8ff
Free Clusters  :                  0x0000000030a814c
Total Reserved :                  0x00000000000010f0
Bytes Per Sector  :               512
Bytes Per Physical Sector :       512
Bytes Per Cluster :               4096
Bytes Per FileRecord Segment    : 1024
Clusters Per FileRecord Segment : 0
Mft Valid Data Length :           0x0000000015380000
Mft Start Lcn  :                  0x00000000000c0000
Mft2 Start Lcn :                  0x0000000000000010
Mft Zone Start :                  0x0000000001ef6ea0
Mft Zone End   :                  0x0000000001f036c0
Max Device Trim Extent Count :    0
Max Device Trim Byte Count :      0x0
Max Volume Trim Extent Count :    62
Max Volume Trim Byte Count :      0x40000000
Resource Manager Identifier :     592B3E69-830B-11E0-B313-C2733971D86C
```

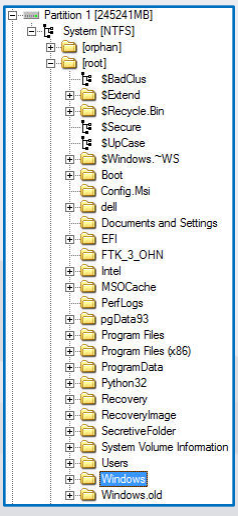


Resilient File System (ReFS) for Storage Pools

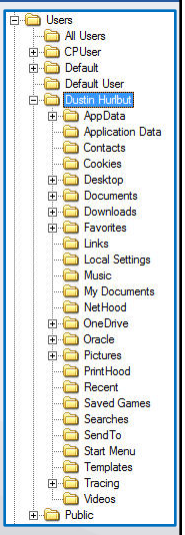
SYNTRICATE

File Structure

SYNTRICATE



- The default root structure is similar to previous versions since Vista
- The user file system profile is also similar
- The now familiar UAC security from Vista is also present

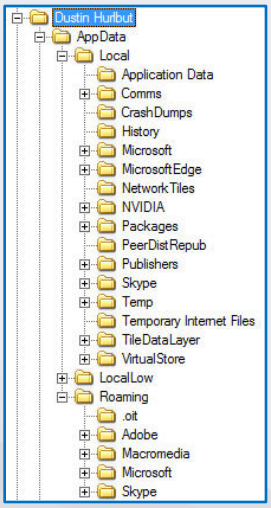


SYNTRICATE

File Structure

SYNTRICATE

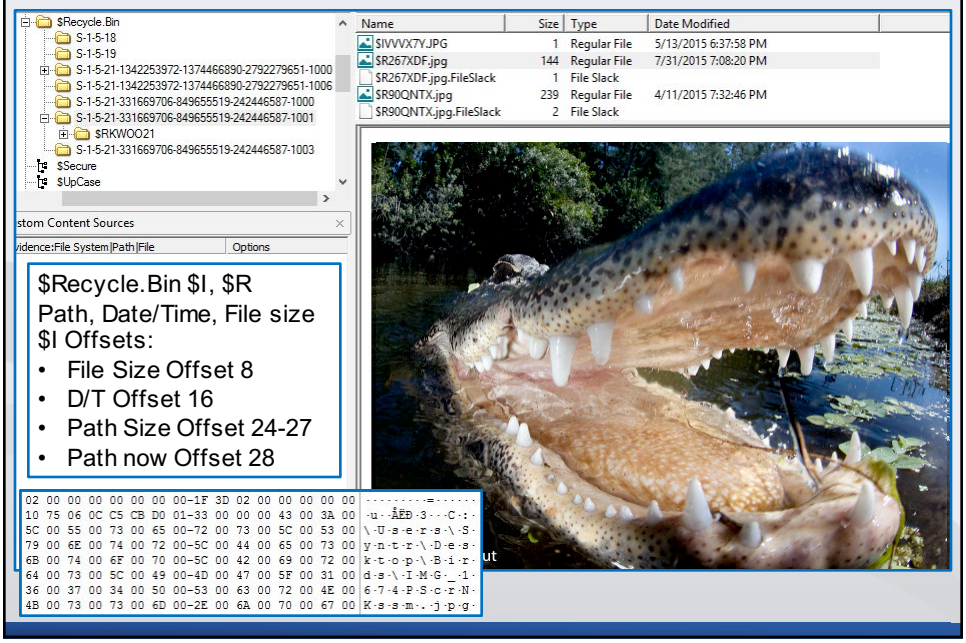
- As with previous versions since Vista, the majority of artifacts for users are in the AppData folder under either:
  - Local
  - Roaming



SYNTRICATE

Recycle Bin

SYNTRICATE



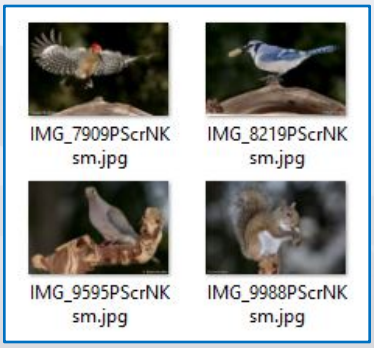
$Recycle.Bin $I, $R
Path, Date/Time, File size
$I Offsets:

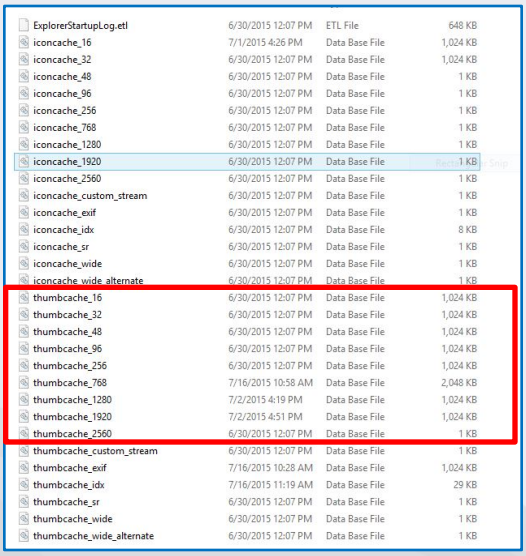
- File Size Offset 8
- D/T Offset 16
- Path Size Offset 24-27
- Path now Offset 28

Thumbnail Cache

SYNTRICATE

- Additional sizes appear to be available for Thumbnail Cache
- Can still be data carved





C:\User\<username>\AppData\Local\Microsoft\Windows\Explorer

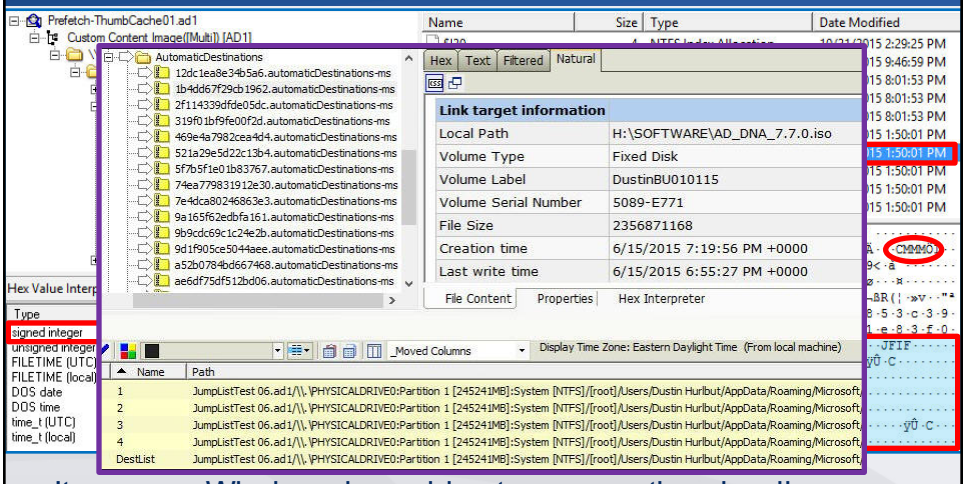
Thumbnail Cache

SYNTRICATE

- Same location as Win 7/8
- Offsets from CMMM header
  - Record Entry size Offset 4
  - Size of thumbnail Offset 24
  - File ID Offset 56
  - No extension information

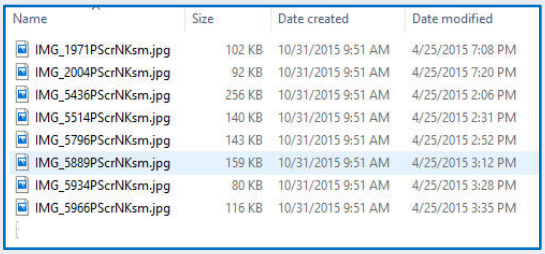

```
00000 43 4D 4D 4D 20 00 00 00-06 00 00 00 00 00 00 00 CMMM ............
00010 18 00 00 00 06 1A 0E 00-43 4D 4D 4D 46 89 02 00 ........CMMMF...
00020 AE 9D 37 8C 59 07 7A 71-20 00 00 00 00 00 00 00 ®·7·Y·zq ........
00030 E7 88 02 00 00 05 00 00-D0 02 00 00 00 00 00 00 ç.......Ð.......
00040 DD 53 66 F4 22 DA 86 24-04 6F 6B 4A 0C BC 25 81 ÝSfô"Ú·$·okJ·¼%·
00050 37 00 31 00 37 00 61 00-30 00 37 00 35 00 39 00 7·1·7·a·0·7·5·9·
00060 38 00 63 00 33 00 37 00-39 00 64 00 61 00 65 00 8·c·3·7·9·d·a·e·
00070 FF D8 FF E0 00 10 4A 46-49 46 00 01 01 01 00 00 ÿØÿà··JFIF......
00080 00 00 00 00 FF DB 00 43-00 04 03 03 04 03 04 07 ····ÿÛ·C........
```

Thumbnail Cache Temp Files

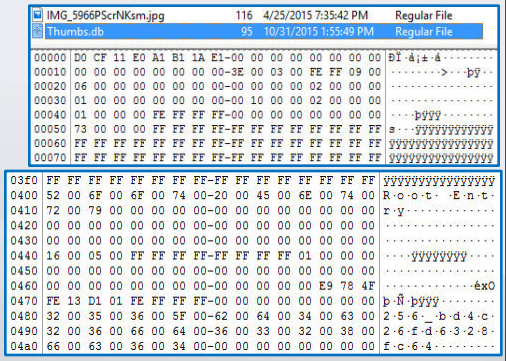


- It appears Windows is caching temporary thumbnails
- File was carve **Full sized graphic screen capture**
- Not a thumbnail size

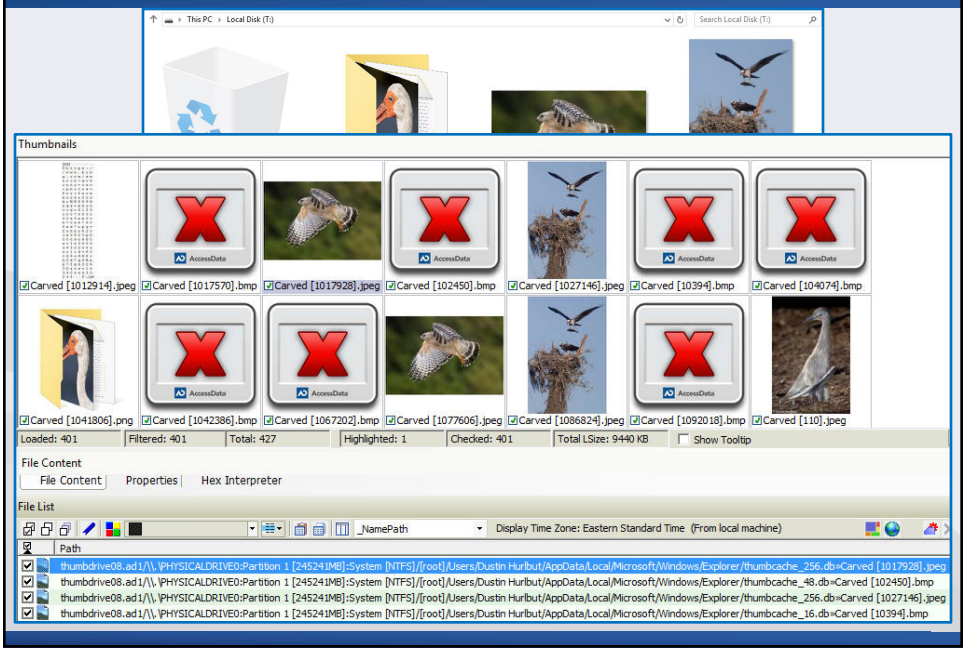
Windows 10 Thumbs.db



- Thumbs.db is created when another machine views the folder in a thumbnail view
- Similar to Win7 and 8
- Modification date indicates when folder was last viewed by any other machine

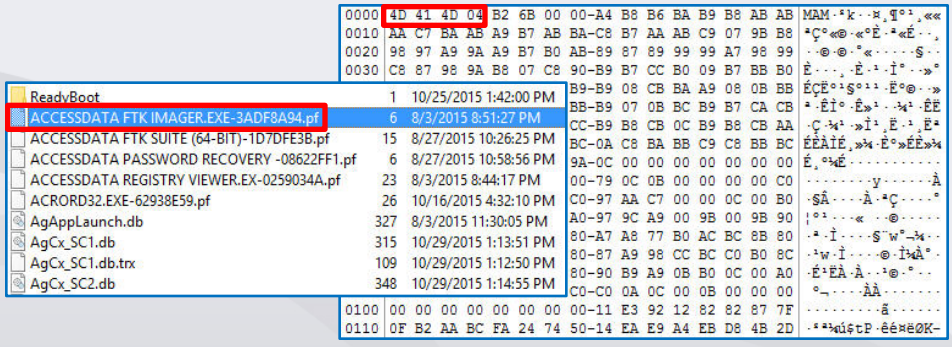


Thumbnail Cache - Encryption



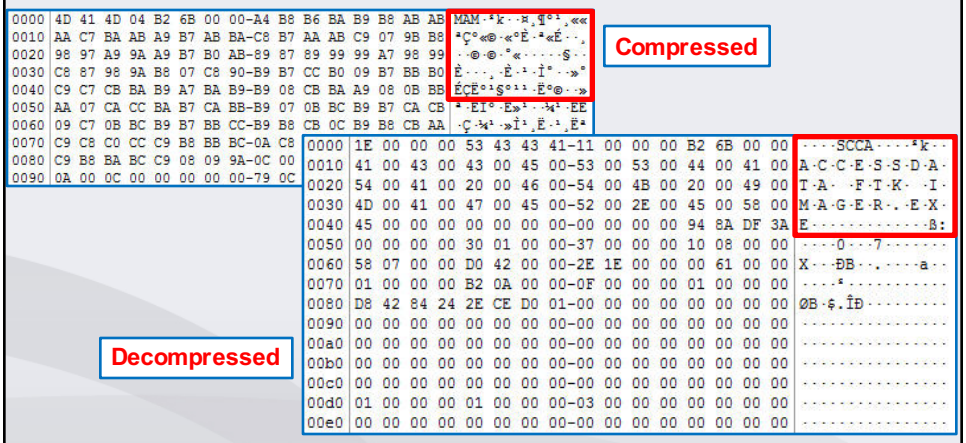
Prefetch Files – Compression

- Compressed with LZExpress Huffman compression
- Header 0x 4D 41 4D 04



Prefetch Files–Decompression

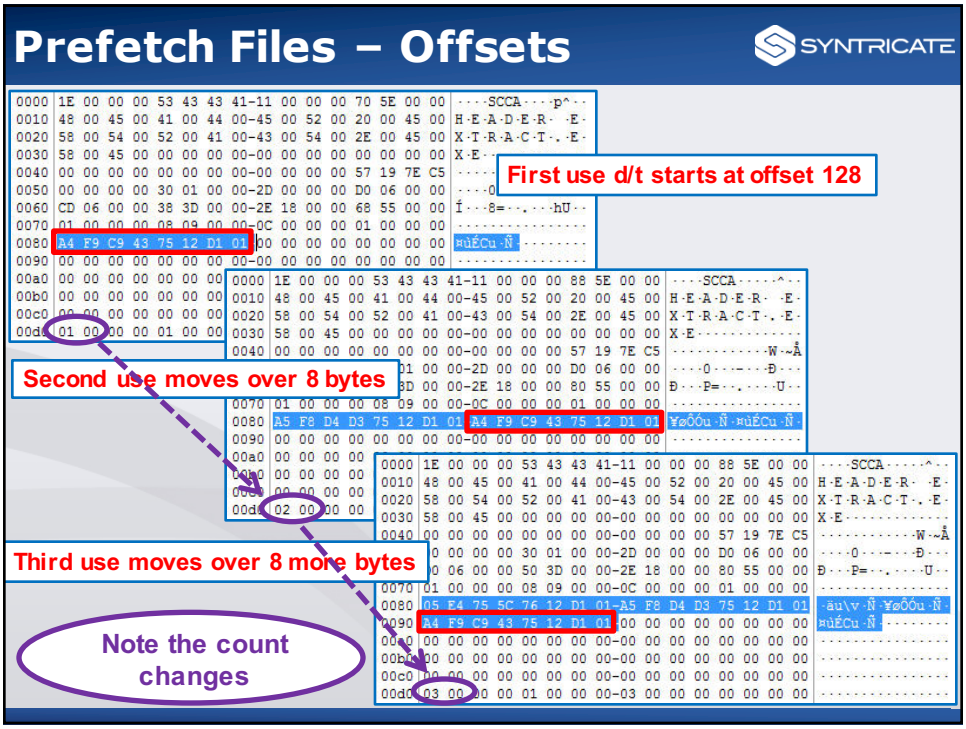
SYNTRICATE



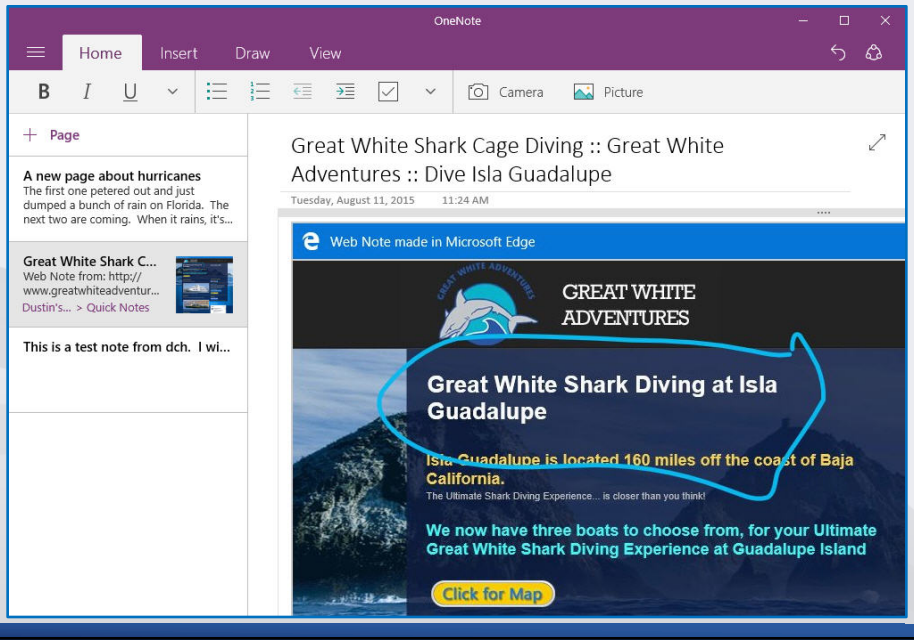
- Decompression using Python script
- Script written by Francesco Picasso

Prefetch Files – Offsets

SYNTRICATE

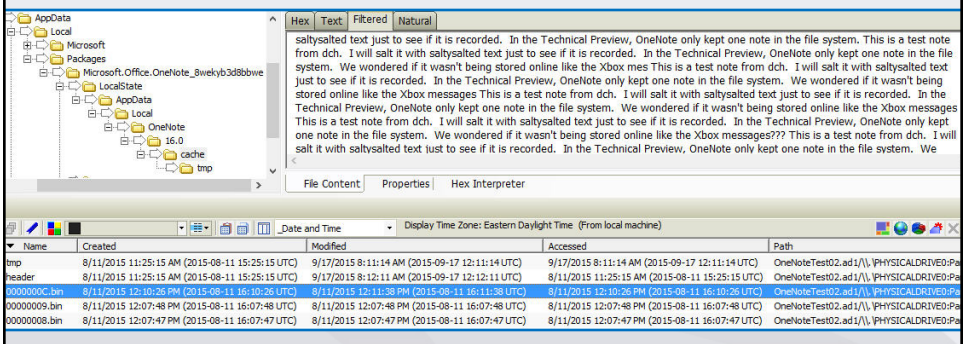


OneNote



OneNote BIN Files

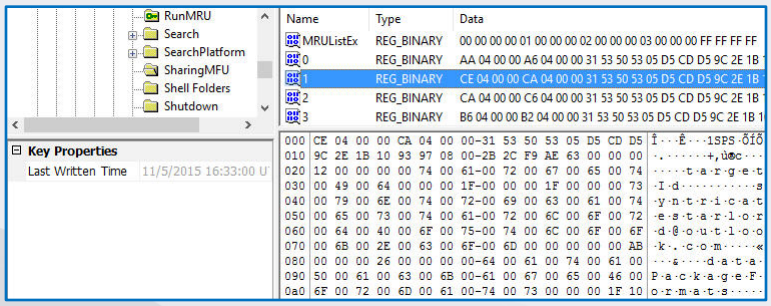
- OneNote stores data in .bin files
- Graphics may occupy an entire .bin
- Graphics may be together with text

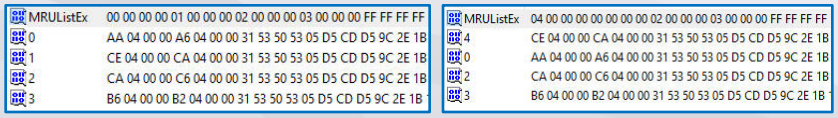


C:\Users\<username>\AppData\Local\Packages\<OneNote>\16.0\cache

OneNote – ShareMFU

- This MRU is tracking shares from OneNote



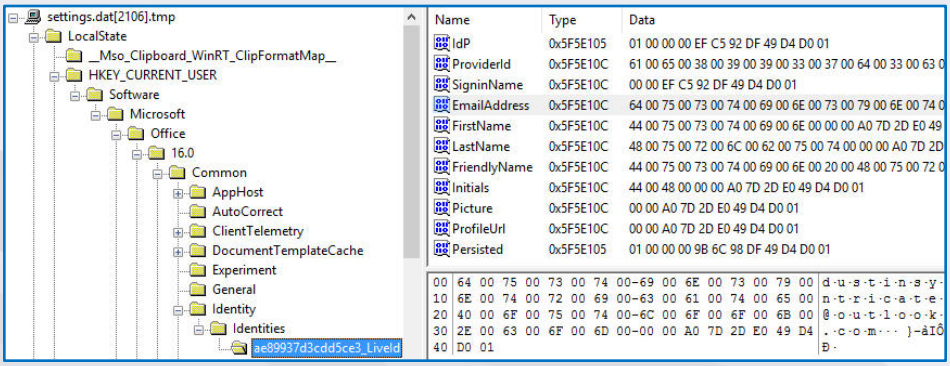


OneNote MRUListEx anomaly

NTUSER.DAT\SOFTWARE\Microsoft\Windows\Current Version\Explorer\SharingMFU

OneNote – Settings.dat

- Settings.dat identity information



C:\Users\<username>\AppData\Local\Packages\<onenote>\Settings

File Explorer – Tracking

SYNTRICATE

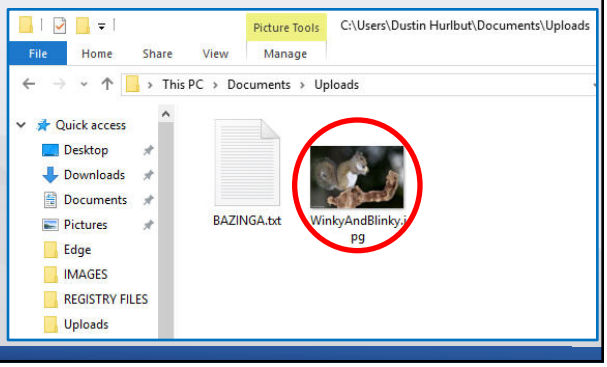
Name	Date created	Date modified	Date accessed
System Volume Information	8/12/2015 10:35 PM		
ff00FEslide.jpg	8/13/2015 3:22 PM	8/13/2015 3:18 PM	8/13/2015 12:00 AM
WinkyAndBlinky.jpg	8/13/2015 12:38 PM	4/18/2015 10:01 PM	8/13/2015 12:00 AM

Created on USB from foreign machine

Moved to Win10 System

	Date created	Date modified	Date accessed
BAZINGA.txt	8/13/2015 1:00 PM	8/13/2015 1:00 PM	8/13/2015 1:00 PM
WinkyAndBlinky.jpg	8/13/2015 12:48 PM	4/18/2015 10:01 PM	8/13/2015 12:48 PM

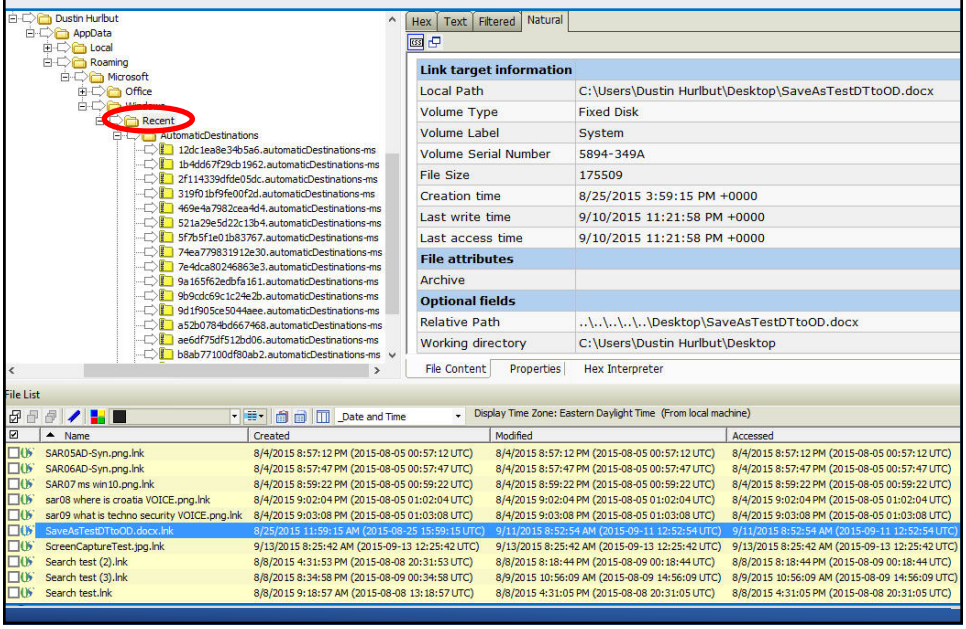
- Note change of Created and Accessed dates and times



SYNTRICATE

Link Files and Jump Lists

SYNTRICATE



Link Files – Tracking

SYNTRICATE

Link target information	
Local Path	C:\Users\Dustin Hurlbut\Documents\Uploads\WinkyAndBlinky.jpg
Volume Type	Fixed Disk
Volume Label	System
Volume Serial Number	5894-349A
File Size	349364
Creation time (UTC)	8/13/2015 4:48:49 PM +0000
Last write time (UTC)	4/19/2015 2:01:18 AM +0000
Last access time (UTC)	8/13/2015 4:48:49 PM +0000
File attributes	
Archive	
Optional fields	
Relative Path	..\..\..\..\..\Documents\Uploads\WinkyAndBlinky.jpg
Working directory	C:\Users\Dustin Hurlbut\Documents\Uploads

- Tracking can still be done with the Link Files
- There have been no obvious changes to their basic format

SYNTRICATE

Link File Basics

SYNTRICATE

Link target information	
Local Path	C:\Users\Dustin Hurlbut\Desktop\SaveAsTestDTtoOD.docx
Volume Type	Fixed Disk
Volume Label	System
Volume Serial Number	5894-349A
File Size	175509
Creation time	8/25/2015 3:59:15 PM +0000
Last write time	9/10/2015 11:21:58 PM +0000
Last access time	9/10/2015 11:21:58 PM +0000
File attributes	
Archive	
Optional fields	
Relative Path	..\..\..\..\..\Desktop\SaveAsTestDTtoOD.docx
Working directory	C:\Users\Dustin Hurlbut\Desktop

Value	Description
0x 00000000	DRIVE_UNKNOWN
0x 00000001	DRIVE_NO_ROOT_DIR
0x 00000002	DRIVE_REMOVABLE
0x 00000003	DRIVE_FIXED
0x 00000004	DRIVE_REMOTE
0x 00000005	DRIVE_CDROM
0x 00000006	DRIVE_RAMDISK

Hex Value Interpreter

Type	Size	Value
signed integer	1-8	175,509
unsigned integer	1-8	175,509

Offset 44-51

Volume Type Designators

```
000 4C 00 00 00 01 14 02 00-00 00 00 00 C0 00 00 00 46 L...........À...F
010 00 00 00 00 46 9B 00 00-00 20 00 00 00 60 DD C3 FD ....F.... ...`ÝÃý
020 4E DF D0 01 14 83 9A 08-1F E5 D0 01 2A AA 98 7D NßÐ....}.iÐ.*ª.}
030 1F E5 D0 01 95 9A 08 02-00 00 00 00 01 00 00 00 .iÐ.•.....
040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 14 00 ..........È...
050 1F 50 E0 4F D0 20 EA 3A-69 10 A7 D8 08 00 2B 30 .PàOÐ ê:i.§ø..+0
060 30 9D 3A 00 2E 80 3A CC-1F E5 2C 2B 4C 42 B0 29 0.:...:Ì¿',ÛLB°)
070 17 7F E9 9A 87 C6 41 26-00-01 00 25 00 FF BE 11 00 ..éšÆA&...%.ÿ¾..
080 00 00 90 C9 3A 87 2C CE-D0 01 6F DD 3B 67 90 EC ...É:.ÎÐ.oÝ;g.ì
090 D0 01 6F DD 3B 67 90 EC-D0 01 14 00 78 00 32 00 Ð.oÝ;g.ìÐ...x.2.
0a0 35 AD 02 00 2A 47 C0 BA-20 00 53 41 56 45 41 53 5-..*GÀº .SAVEAS
0b0 7E 31 2E 44 4F 43 00 00-5C 00 00 00 00 00 EF BE ~1.DOC..\.....i¾
0c0 19 47 68 7F 2A 47 C0 BA-2E 00 00 00 DD 16 01 00 .Gh.*GÀº....Ý...
0d0 00 00 0F 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0e0 00 00 D6 31 53 00 53 00-61 00 76 00 65 00 41 00 ..Ö1S.S.a.v.e.A.
0f0 73 00 54 00 65 00 73 00-74 00 44 00 54 00 74 00 s.T.e.s.t.D.T.t.
100 6F 00 4F 00 44 00 2E 00-64 00 6F 00 63 00 78 00 o.O.D...d.o.c.x.
110 00 00 1C 00 00 00 6A 00-00 00 1C 00 00 00 01 00 ......j.........
120 00 00 1C 00 00 00 33 00-00 00 00 00 00 00 69 00 ......3.......i.
130 00 00 17 00 00 00 03 00-00 00 9A 34 94 58 10 00 ...........4.X..
140 00 00 53 79 73 74 65 6D-00 43 3A 5C 55 73 65 72 ..System.C:\User
150 73 5C 44 75 73 74 69 6E-20 48 75 72 6C 62 75 74 s\Dustin Hurlbut
160 5C 44 65 73 6B 74 6F 70-5C 53 61 76 65 41 73 54 \Desktop\SaveAsT
170 65 73 74 44 54 74 6F 4F-44 2E 64 6F 63 78 00 00 estDTtoOD.docx..
180 2C 00 2E 00 2E 00 5C 00-2E 00 2E 00 5C 00 2E 00 ,.....\.....\...
190 2E 00 5C 00 2E 00 2E 00-5C 00 2E 00 2E 00 5C 00 ..\.....\.....\.
1a0 44 00 65 00 73 00 6B 00-74 00 6F 00 70 00 5C 00 D.e.s.k.t.o.p.\.
1b0 53 00 61 00 76 00 65 00-41 00 73 00 54 00 65 00 S.a.v.e.A.s.T.e.
1c0 73 00 74 00 44 00 54 00-74 00 6F 00 4F 00 44 00 s.t.D.T.t.o.O.D.
1d0 2E 00 64 00 6F 00 63 00-78 00 1F 00 43 00 3A 00 ..d.o.c.x...C.:.
1e0 5C 00 55 00 73 00 65 00-72 00 73 00 5C 00 44 00 \.U.s.e.r.s.\.D.
1f0 75 00 73 00 74 00 69 00-6E 00 20 00 48 00 75 00 u.s.t.i.n. .H.u.
200 72 00 6C 00 62 00 75 00-74 00 5C 00 44 00 65 00 r.l.b.u.t.\.D.e.
210 73 00 6B 00 74 00 6F 00-70 00 60 00 00 00 03 00 s.k.t.o.p.`.....
```

SYNTRICATE

Distributed Link Tracking

SYNTRICATE

```
C:\WINDOWS\system32\cmd.exe

C:\LinkTest>fsutil objectid query ObjID.txt
Object ID :         5cd22d31a89ae5119bfaa4badbba220f
BirthVolume ID :    0a874aede0ae614e93631190fd99c7e5
BirthObjectId ID :  5cd22d31a89ae5119bfaa4badbba220f
Domain ID :         00000000000000000000000000000000

C:\LinkTest>
```

Current Location

- Object ID
- Volume ID

$MFT 347,648 Regular File 5/20/2011 6:05:...

```
00000c00  46 49 4C 45 30 00 03 00-56 40 65 A4 00 00 00 00  FILE0···V@e¤····
00000c10  03 00 01 00 38 00 01 00-98 01 00 00 00 04 00 00  ····8···˜·····
00000c20  00 00 00 00 00 00 00 00-07 00 00 00 03 00 00 00  ····************
00000c30  1F 6A 00 00 00 00 00 00-10 00 00 00 60 00 00 00  ·j··········`···
00000c40  00 00 18 00 00 00 00 00-48 00 00 00 18 00 00 00  ········H·******
00000c50  1E A7 53 92 18 17 CC 01-1E A7 53 92 18 17 CC 01  ·§S···Ì··§S···Ì·
00000c60  1E A7 53 92 18 17 CC 01-1E A7 53 92 18 17 CC 01  ·§S···Ì··§S···Ì·
00000c70  06 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ****************
00000c80  00 00 00 00 01 01 00 00-00 00 00 00 00 00 00 00  ****************
00000c90  00 00 00 00 00 00 00 00-30 00 00 00 68 00 00 00  ********0···h···
00000ca0  00 00 18 00 00 00 01 00-50 00 00 00 18 00 01 00  ********P·******
00000cb0  05 00 00 00 00 00 05 00-1E A7 53 92 18 17 CC 01  ··********§S···Ì·
00000cc0  1E A7 53 92 18 17 CC 01-1E A7 53 92 18 17 CC 01  ·§S···Ì··§S···Ì·
00000cd0  1E A7 53 92 18 17 CC 01-00 00 00 00 00 00 00 00  ·§S···Ì·********
00000ce0  00 00 00 00 00 00 00 00-06 00 00 00 00 00 00 00  ****************
00000cf0  07 03 24 00 56 00 6F 00-6C 00 75 00 6D 00 65 00  ··$·V·o·l·u·m·e·
00000d00  40 00 00 00 28 00 00 00-00 00 00 00 00 00 06 00  @···(···********
00000d10  10 00 00 00 18 00 00 00-0A 87 4A ED E0 AE 61 4E  ********·‡JíàaN
00000d20  93 63 11 90 FD 99 C7 E5-60 00 00 00 28 00 00 00  ·c··ý·Çå`···(···
00000d30  00 00 18 00 00 00 04 00-0C 00 00 00 18 00 00 00  ****************
```

- Object ID assigned to each file
  - Stored in .lnk file and potentially the $MFT
- Volume ID assigned to individual drives
  - Located in $Volume $MFT record entry at offset 24 from the 0x 40 00 00 00 attribute

Volume must be formatted in NTFS for this artifact to be present

Link File Basics – Back End

SYNTRICATE

$MFT 347,648 Regular File 5/20/2011 6:05:58 PM

```
00a49000  46 49 4C 45 30 00 03 00-CE FD 68 B4 03 00 00 00  FILE0···Îýh´····
00a49010  2E 00 01 00 38 00 01 00-60 01 00 00 00 04 00 00  .···8···`·******
00a49020  00 00 00 00 00 00 00 00-06 00 00 00 24 29 00 00  ************$)··
00a49030  03 00 00 00 00 00 00 00-10 00 00 00 60 00 00 00  ************`···
00a49040  00 00 00 00 00 00 00 00-48 00 00 00 18 00 00 00  ********H·******
00a49050  52 78 30 B2 93 41 D1 01-28 E9 A9 BD 93 41 D1 01  Rx0²·AÑ·(é©½·AÑ·
00a49060  28 E9 A9 BD 93 41 D1 01-52 78 30 B2 93 41 D1 01  (é©½·AÑ·Rx0²·AÑ·
00a49070  20 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ****************
00a49080  00 00 00 00 F6 1C 00 00-00 00 00 00 00 00 00 00  ····ö···********
00a49090  38 B9 59 E6 00 00 00 00-30 00 00 00 70 00 00 00  8¹Yæ····0···p···
00a490a0  00 00 00 00 00 00 04 00-54 00 00 00 18 00 01 00  ********T·******
00a490b0  42 18 00 00 00 00 79 00-52 78 30 B2 93 41 D1 01  B·····y·Rx0²·AÑ·
00a490c0  52 78 30 B2 93 41 D1 01-52 78 30 B2 93 41 D1 01  Rx0²·AÑ·Rx0²·AÑ·
00a490d0  52 78 30 B2 93 41 D1 01-00 00 00 00 00 00 00 00  Rx0²·AÑ·********
00a490e0  00 00 00 00 00 00 00 00-20 00 00 00 00 00 00 00  ******** *******
00a490f0  09 03 4F 00 62 00 6A 00-49 00 44 00 2E 00 74 00  ··O·b·j·I·D·.·t·
00a49100  78 00 74 00 00 00 00 00-40 00 00 00 28 00 00 00  x·t·····@···(···
00a49110  00 00 00 00 00 00 05 00-10 00 00 00 18 00 00 00  ****************
00a49120  5C D2 2D 31 A8 9A E5 11-9B FA A4 BA DB BA 22 0F  \Ò-1¨šå·›ú¤ºÛº"·
00a49130  80 00 00 00 28 00 00 00-00 00 18 00 00 00 01 00  ····(···********
00a49140  0C 00 00 00 18 00 00 00-48 65 6C 6C 6F 20 57 6F  ********Hello Wo
00a49150  72 6C 64 21 00 00 00 00-FF FF FF FF 82 79 47 11  rld!····ÿÿÿÿ·yG·
```

- Three common ways to look up the Object Identifier:
  - fsutil command
  - $MFT entry for the document
  - Back end of the document's link file

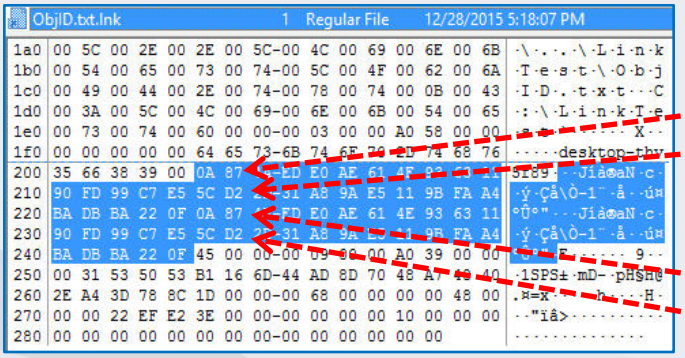
- Four GUIDs at the end of the link file
- Describe the object, its current location and past location

ObjID.txt.lnk 1 Regular File 12/28/2015 5:18:07 PM

```
1a0  00 5C 00 2E 00 2E 00 5C-00 4C 00 69 00 6E 00 6B  ·\·.·.·\·L·i·n·k
1b0  00 54 00 65 00 73 00 74-00 5C 00 4F 00 62 00 6A  ·T·e·s·t·\·O·b·j
1c0  00 49 00 44 00 2E 00 74-00 78 00 74 00 0B 00 43  ·I·D·.·t·x·t···C
1d0  00 3A 00 5C 00 4C 00 69-00 6E 00 6B 00 54 00 65  ·:·\·L·i·n·k·T·e
1e0  00 73 00 74 00 60 00 00-00 03 00 00 A0 58 00 00  ·s·t·`·····X··
1f0  00 00 00 00 00 64 65 73-6B 74 6F 70 2D 74 68 76  ·····desktop-thv
200  35 66 38 39 00 0A 87 4A-ED E0 AE 61 4E 93 63 11  5f89···JíàaN·c·
210  90 FD 99 C7 E5 5C D2 2D-31 A8 9A E5 11 9B FA A4  ·ý·Çå\Ò-1¨·å··ú¤
220  BA DB BA 22 0F 0A 87 4A-ED E0 AE 61 4E 93 63 11  ºÛº"···JíàaN·c·
230  90 FD 99 C7 E5 5C D2 2D-31 A8 9A E5 11 9B FA A4  ·ý·Çå\Ò-1¨·å··ú¤
240  BA DB BA 22 0F 45 00 00-00 09 00 00 A0 39 00 00  ºÛº"·E·····  9··
250  00 31 53 50 53 B1 16 6D-44 AD 8D 70 48 A7 48 40  ·1SPS±·mD-·pH§H@
260  2E A4 3D 78 8C 1D 00 00-00 68 00 00 00 00 48 00  .¤=x·····h····H·
270  00 00 22 EF E2 3E 00 00-00 00 00 00 10 00 00 00  ··"ïâ>··********
280  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ****************
```

Link File Basics – Back End

SYNTRICATE



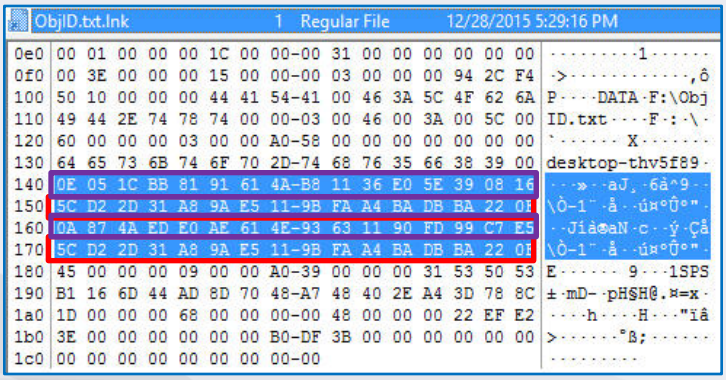
- Current Location
  - Volume ID
  - Object ID
- Birth Location
  - Volume ID
  - Object ID

Static file that has not been moved since creation

200	35 66 38 39 00	0A 87 4A-ED E0 AE 61 4E 93 63 11	5f89···Jíà©aN·c·
210	90 FD 99 C7 E5	5C D2 2D-31 A8 9A E5 11 9B FA A4	·ý·Çå\Ò-1¨·å··ú¤
220	BA DB BA 22 0F	0A 87 4A-ED E0 AE 61 4E 93 63 11	°Û°"···Jíà©aN·c·
230	90 FD 99 C7 E5	5C D2 2D-31 A8 9A E5 11 9B FA A4	·ý·Çå\Ò-1¨·å··ú¤
240	BA DB BA 22 0F	45 00 00-00 09 00 00 A0 39 00 00	°Û°"·E·····9··

Link File Basics – Moved File

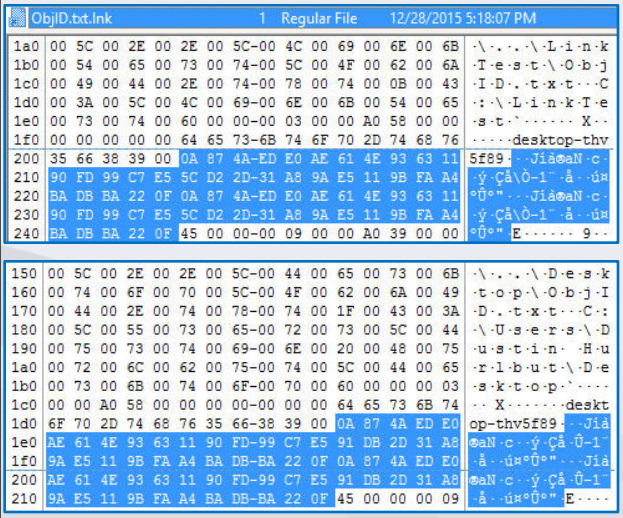
SYNTRICATE



- Cut and Paste to another volume (F Drive)
  - Different Volume ID starting with 0x 0E 05 1C BB….
  - Same Object ID value starting with 0x 5C D2 2D 31….
  - Note, the old Birth Volume ID retained 0x 0A 87 4A ED….

Link File Basics – Moved File

SYNTRICATE

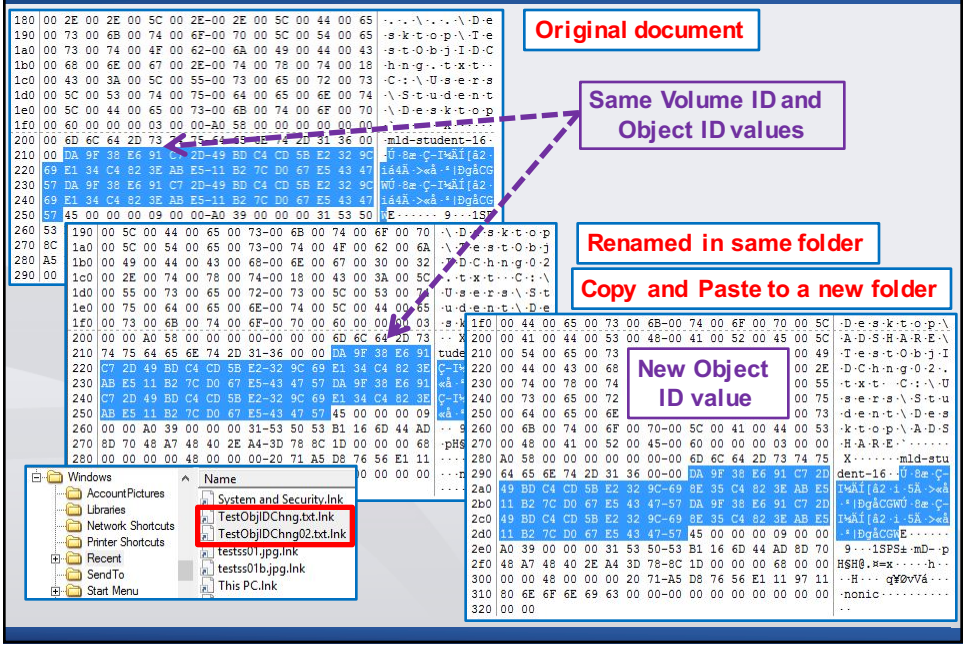


- Copy and Paste to a different folder on the same volume
  - Retains same Volume ID
  - New Object ID assigned to new document

At this point they could be the same file with the same name, or a different file with the same name. A hash check of the files can determine the difference

Renamed File

SYNTRICATE



USB Storage Devices

SYNTRICATE

100	50	10	00	00	00	44	75	73-74	69	6E	42	55	30	31	30	P····DustinBU010
110	31	31	35	00	47	3A	5C	4F-62	6A	49	44	2E	74	78	74	115·G:\ObjID.txt
120	00	00	03	00	47	00	3A	00-5C	00	60	00	00	00	03	00	····G·:·\·`·····
130	00	A0	58	00	00	00	00	00-00	00	64	65	73	6B	74	6F	·X·····deskto
140	70	2D	74	68	76	35	66	38-39	00	A2	E8	9F	4B	A6	71	p-thv5f89·¢è·K¦q
150	8E	44	A4	33	20	CE	DA	F0-1D	A4	D0	D7	2D	31	A8	9A	·D¤3 ÎÚð·¤Ð×-1¨·
160	E5	11	9B	FA	A4	BA	DB	BA-22	0F	A2	E8	9F	4B	A6	71	å··ú¤ºÛº"··¢è·K¦q
170	8E	44	A4	33	20	CE	DA	F0-1D	A4	D0	D7	2D	31	A8	9A	·D¤3 ÎÚð·¤Ð×-1¨·
180	E5	11	9B	FA	A4	BA	DB	BA-22	0F	45	00	00	00	09	00	å··ú¤ºÛº"·E·····
190	00	A0	39	00	00	00	31	53-50	53	B1	16	6D	44	AD	8D	·9···1SPS±·mD-·
1a0	70	48	A7	48	40	2E	A4	3D-78	8C	1D	00	00	00	68	00	pH§H@.¤=x·····h·
1b0	00	00	00	48	00	00	00	7F-28	A4	1A	00	00	00	00	00	···H····(¤·····
1c0	00	10	00	00	00	00	00	00-00	00	00	00	00	00	00	00	·····-·-·-·····
1d0	00	00	00													···

Seagate BUP Slim – 2TB

120	00	02	00	00	00	81	6E	97-AE	10	00	00	00	44	55	53	·····n·®····DUS
130	54	49	4E	00	45	3A	5C	4F-62	6A	49	44	2E	74	78	74	TIN·E:\ObjID.txt
140	00	00	03	00	45	00	3A	00-5C	00	60	00	00	00	03	00	····E·:·\·`·····
150	00	A0	58	00	00	00	00	00-00	00	64	65	73	6B	74	6F	·X·····deskto
160	70	2D	74	68	76	35	66	38-39	00	00	00	00	00	00	00	p-thv5f89·····-
170	00	00	00	00	00	00	00	00-00	00	05	D8	2D	31	A8	9A	··········Ø-1¨·
180	E5	11	9B	FA	A4	BA	DB	BA-22	0F	00	00	00	00	00	00	å··ú¤ºÛº"·····-
190	00	00	00	00	00	00	00	00-00	00	05	D8	2D	31	A8	9A	··········Ø-1¨·
1a0	E5	11	9B	FA	A4	BA	DB	BA-22	0F	45	00	00	00	09	00	å··ú¤ºÛº"·E·····
1b0	00	A0	39	00	00	00	31	53-50	53	B1	16	6D	44	AD	8D	·9···1SPS±·mD-·
1c0	70	48	A7	48	40	2E	A4	3D-78	8C	1D	00	00	00	68	00	pH§H@.¤=x·····h·
1d0	00	00	00	48	00	00	00	B0-C7	2D	31	A8	9A	E5	11	9B	···H···°Ç-1¨·å··
1e0	FA	A4	BA	DB	BA	22	0F	00-00	00	00	00	00	00	00	00	ú¤ºÛº"·····-·····
1f0	00	00	00													···

SanDisk Cruzer Blade USB – 2GB

- Portable USB HDD
  - Functions like a HDD
  - Stores a Volume ID in the $Volume 0x 40 00 00 00 attribute in the $MFT
- USB
  - Treated differently, no Volume ID value
  - No $Volume attribute

Different Devices

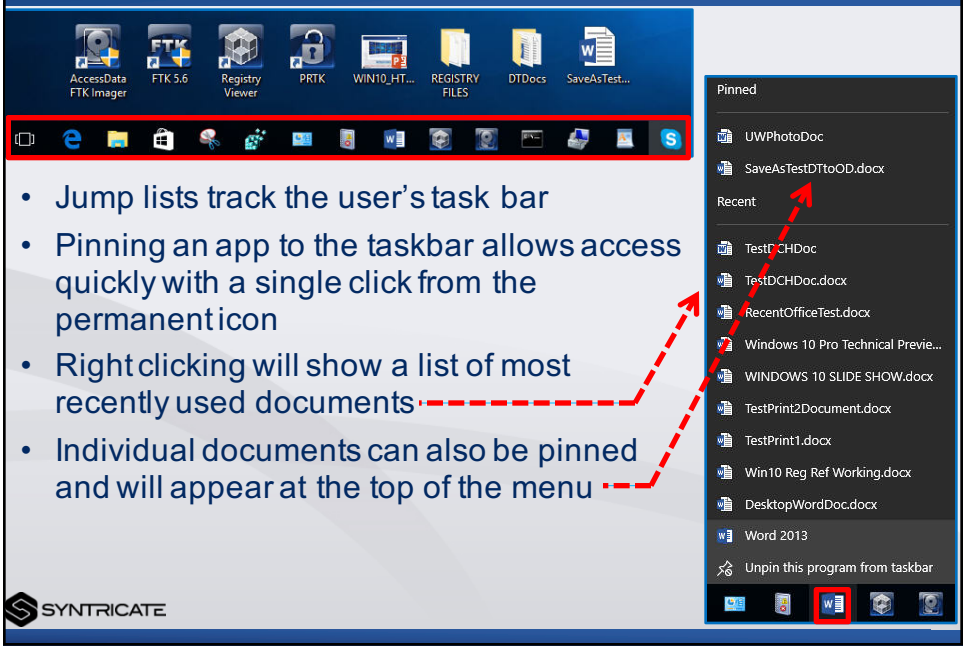
SYNTRICATE

- Cameras
  - No link files created
  - No drive letter assigned
  - No values

- Camera Card (CF)
  - Link file present
  - FAT format – No Values

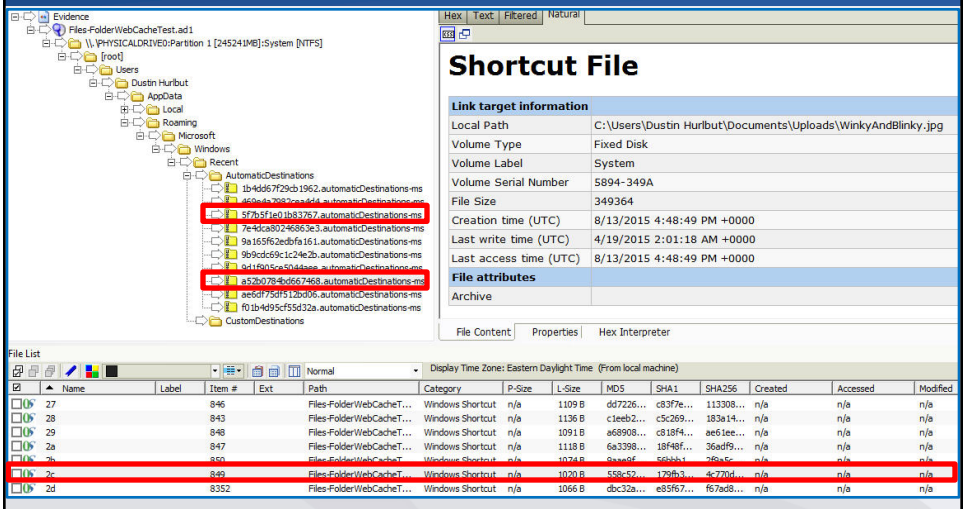
190	00	00	00	00	00	49	00	4D-00	47	00	5F	00	34	00	38	·····I·M·G·_·4·8
1a0	00	38	00	31	00	2E	00	43-00	52	00	32	00	00	00	1C	·8·1·.·C·R·2····
1b0	00	00	00	57	00	00	00	1C-00	00	00	01	00	00	00	1C	···W·····-·····
1c0	00	00	00	38	00	00	00	00-00	00	00	56	00	00	00	1C	···8·····V····
1d0	00	00	00	02	00	00	00	00-00	00	00	10	00	00	00	45	·····-·-·-····E
1e0	4F	53	5F	44	49	47	49	54-41	4C	00	45	3A	5C	44	43	OS_DIGITAL·E:\DC
1f0	49	4D	5C	31	30	30	45	4F-53	35	44	5C	49	4D	47	5F	IM\100EOS5D\IMG_
200	34	38	38	31	2E	43	52	32-00	00	10	00	45	00	3A	00	4881.CR2····E·:·
210	5C	00	44	00	43	00	49	00-4D	00	5C	00	31	00	30	00	\·D·C·I·M·\·1·0·
220	30	00	45	00	4F	00	53	00-35	00	44	00	00	00	00	00	0·E·O·S·5·D·····

Jump Lists



- Jump lists track the user's task bar
- Pinning an app to the taskbar allows access quickly with a single click from the permanent icon
- Right clicking will show a list of most recently used documents
- Individual documents can also be pinned and will appear at the top of the menu

Jump List – Tracking



- Jump Lists are links to documents, objects, and folders
- Standard link files are embedded in the archive files

Jump List App IDs

SYNTRICATE

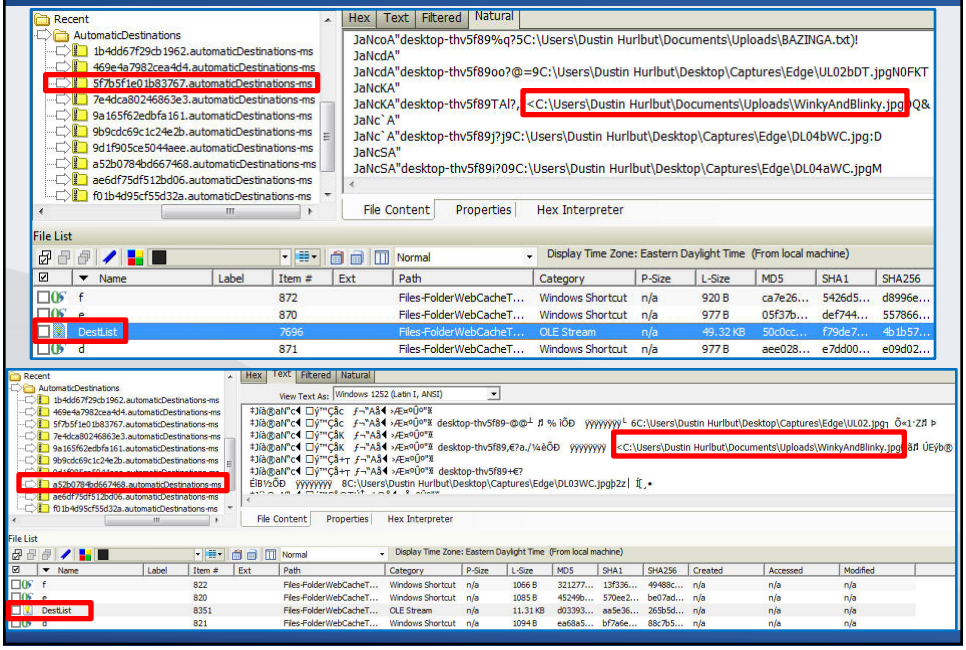
- Applications are identified with a value at the beginning of name
- Apps may have more than one value
  - Type (32-bit versus 64-bit)
  - Version
  - Path
- IDs are generated as a CRC64 value from the path of the app
- Default installations of common apps result in the same values across systems

AutomaticDestinations ID	Application
12dc1ea8e34b5a6	MS Paint
1b4dd67f29cb1962	Windows Explorer Virtual
28c8b86deab549a1	IE Version 11
319f01bf9fe00f2d	MS Access
469e4a7982cea4d4	Wordpad
5f7b5f1e01b83767	File Explorer
7e4dca80246863e3	Control Panel
9a165f62edbfa161	Windows Store
9b9cdc69c1c24e2b	Notepad
9d1f905ce5044aee	Edge Browser
a52b0784bd667468	Windows Photo
ae6df75df512bd06	Zune Music App
b8ab77100df80ab2	Excel 2013
d00655d2aa12ff6d	PowerPoint 2013
de48a32edcbe79e4	Adobe Acrobat Reader
f01b4d95cf55d32a	File Explorer
fb3b0dbfee58fac8	Word 2013

fb3b0dbfee58fac8.automaticDestinations-ms

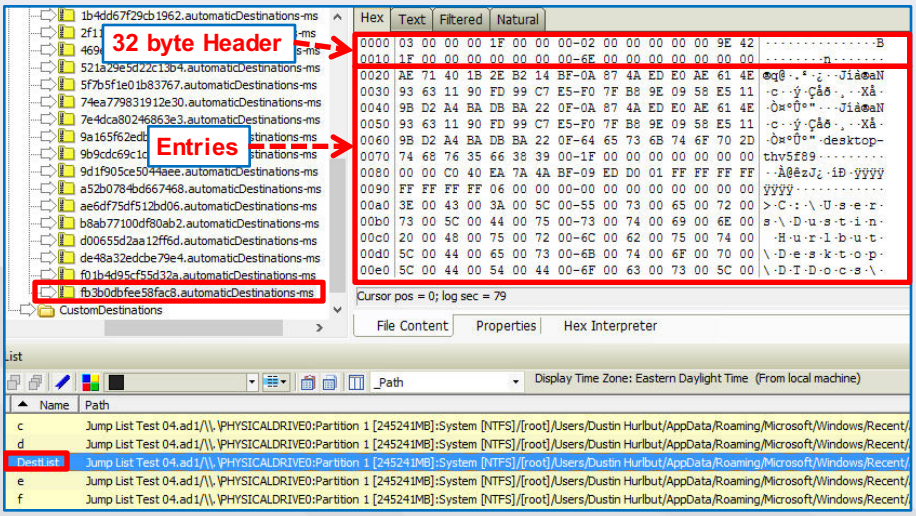
Jump List – DestList

SYNTRICATE



DestList

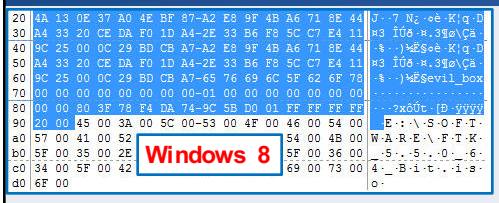
SYNTRICATE



- DestLists are compound files that store records of access
- Track like an MRU, MFU, including dates and times

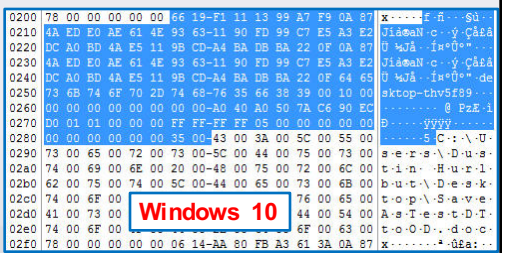
DestList Win7-8 vs. Win10

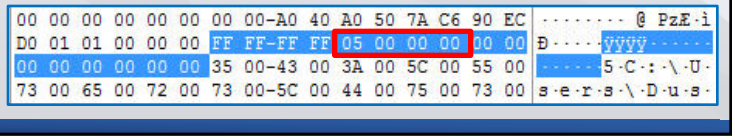
SYNTRICATE



- Windows 7, 8
- 114 bytes from start of record to path string
- No consistent count value

- Windows 10 has 130 bytes from start of record to the path string
- There appears to be a consistent count value within the new 16 bytes
- Offset 116-119



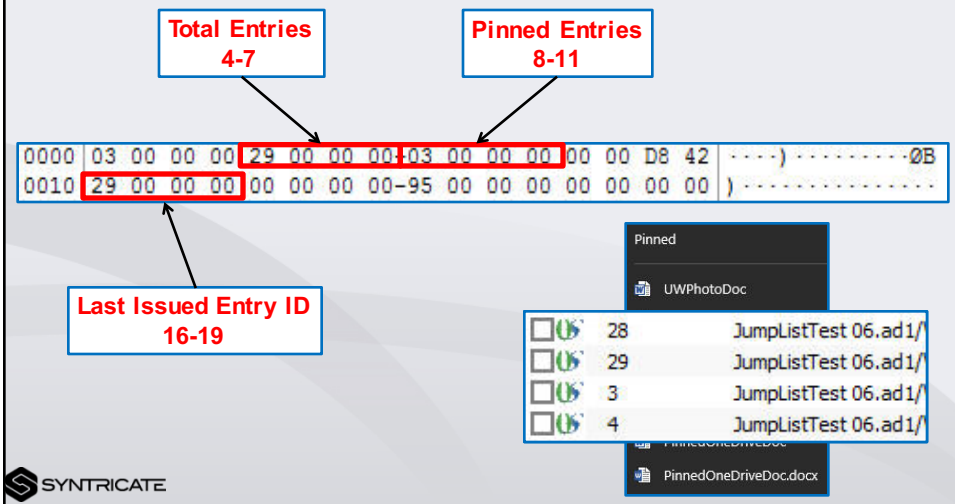


SYNTRICATE

DestList – Header Entries

SYNTRICATE

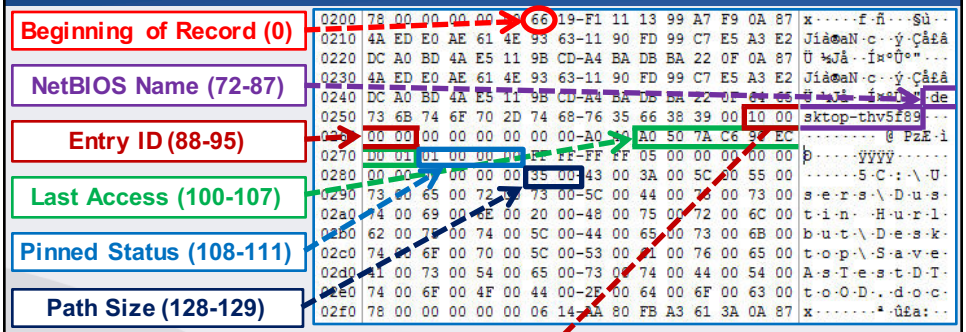
- Each DestList has a 32 byte header
- Header Offsets:



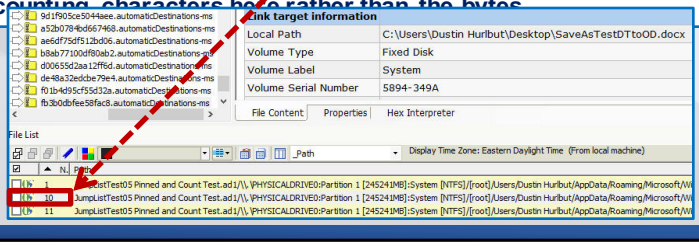
SYNTRICATE

DestList Offsets Windows 10

SYNTRICATE

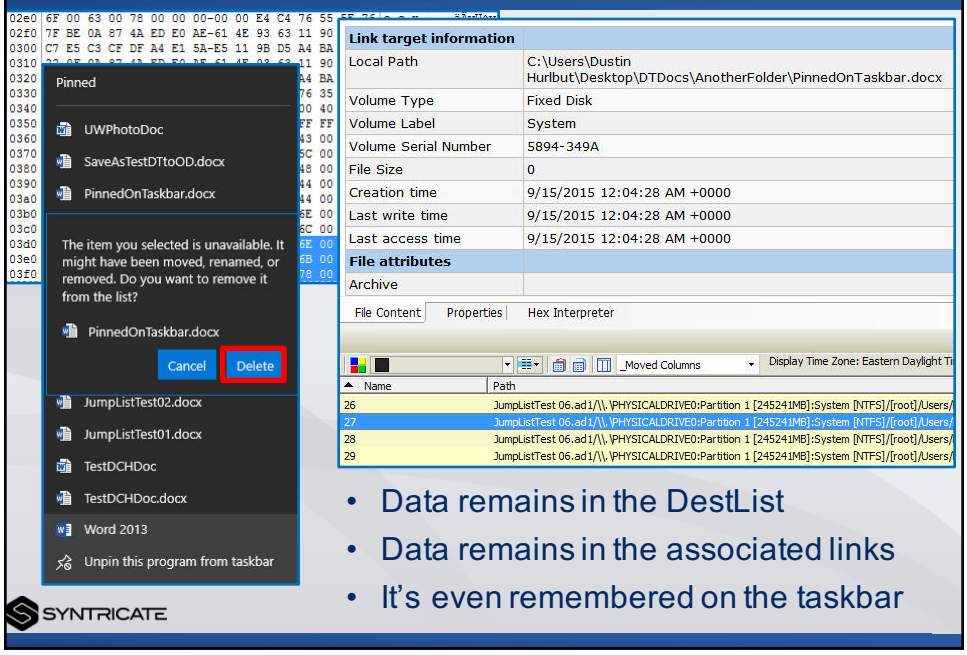


It is odd that the value here is not supporting Unicode. The 0x35 value in the slide = 53 decimal. There are 106 bytes in the path string. It appears Microsoft is counting characters here rather than the bytes.



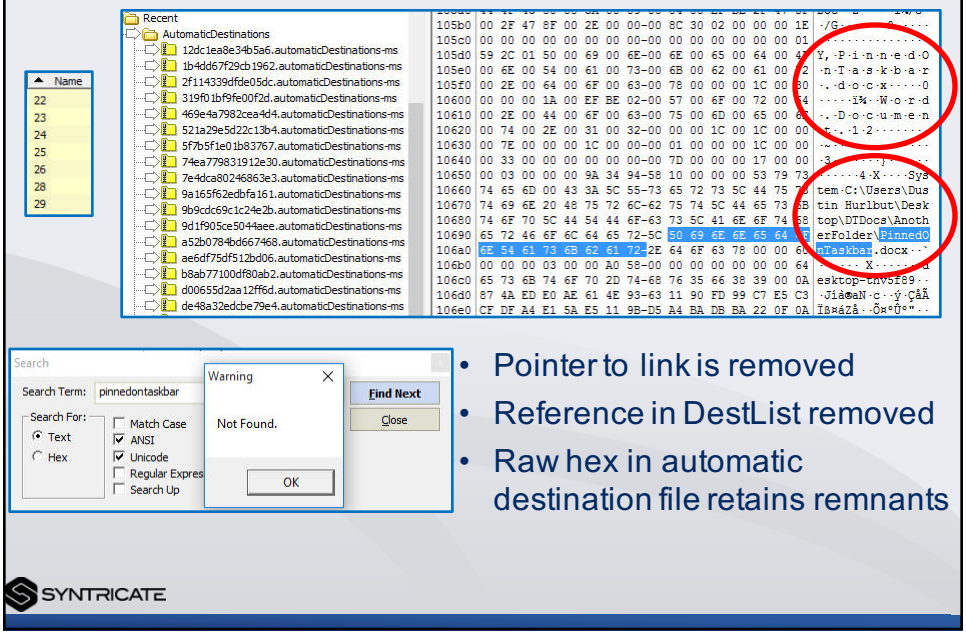
SYNTRICATE

Jump List – Deleted Reference



- Data remains in the DestList
- Data remains in the associated links
- It's even remembered on the taskbar

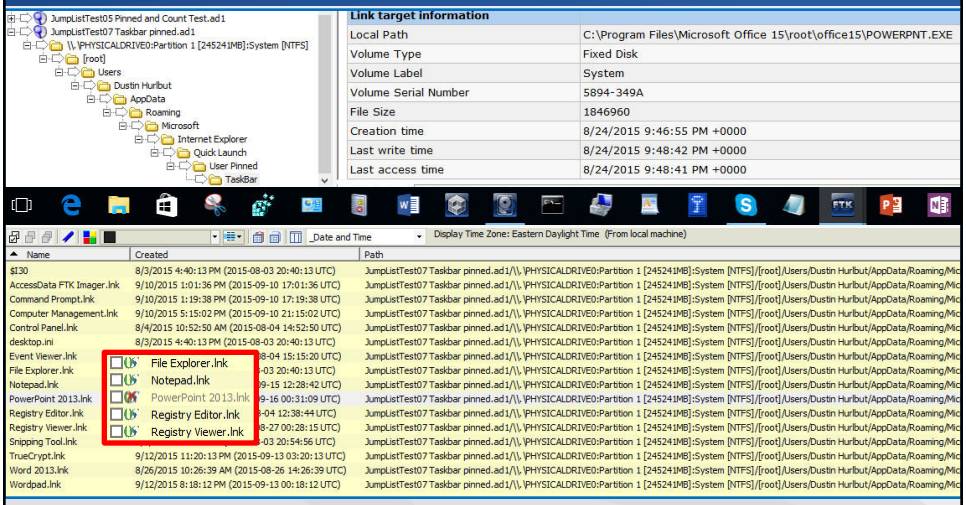
Jump List – Deleted File



- Pointer to link is removed
- Reference in DestList removed
- Raw hex in automatic destination file retains remnants

User Pinned – File System

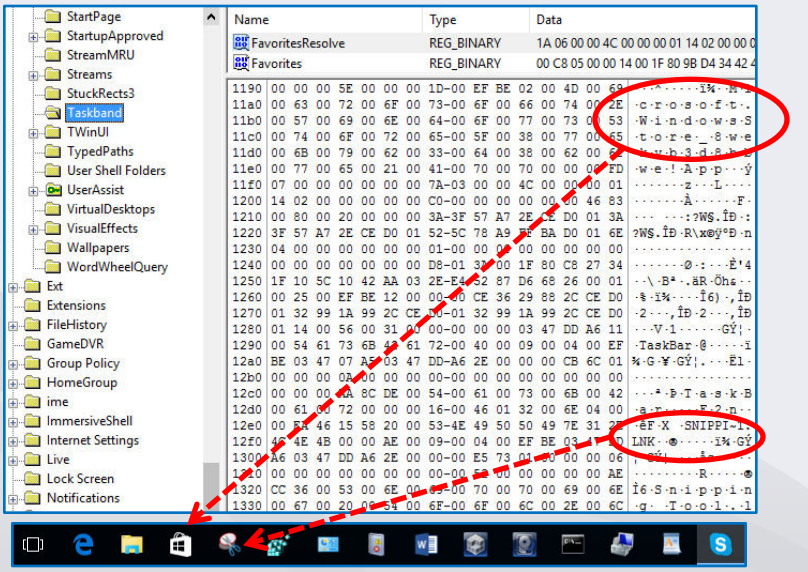
SYNTRICATE



- User pinned apps are also stored in the file system
- Not all show up here (OneNote did not populate)
- Ignore the date inside the link – Created date in file system is when created

Jump Lists – Registry

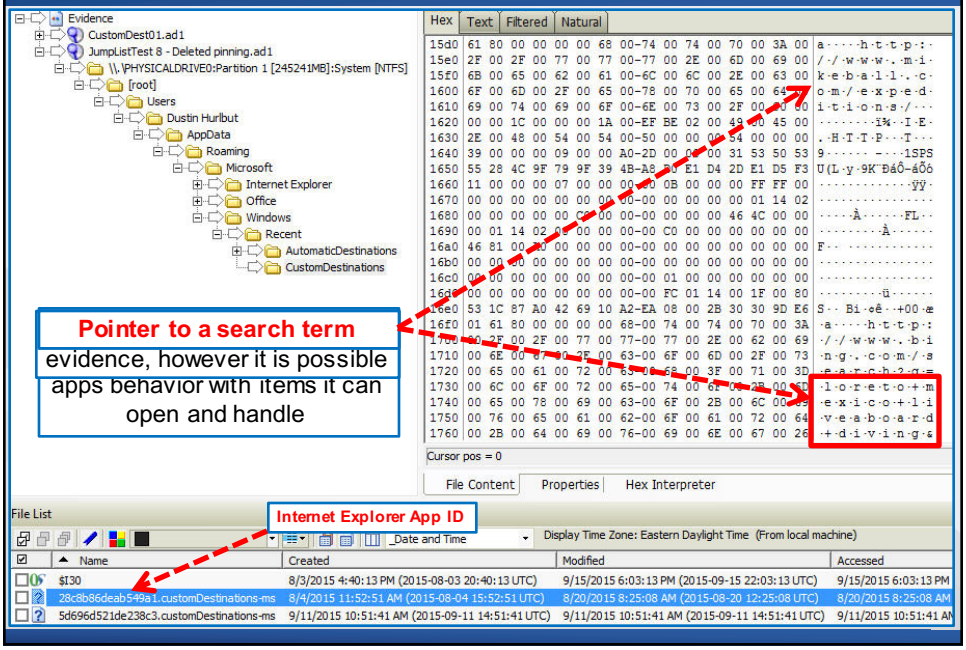
SYNTRICATE



NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Taskband

CustomDestinations

SYNTRICATE



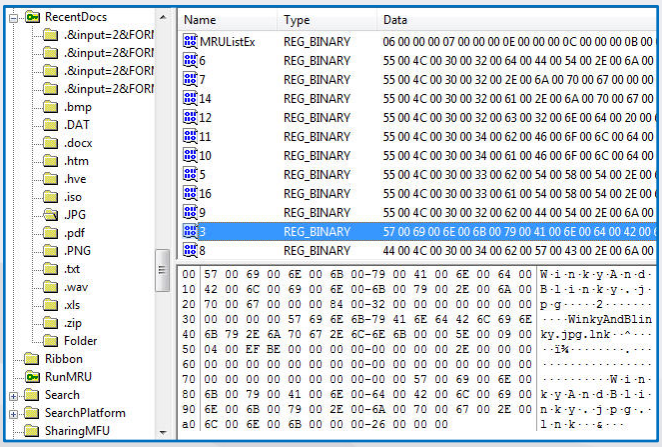
File Explorer – Tracking

SYNTRICATE

Name	Value
Url	Visited: Dustin Hurlbut@file:///C:/Users/Dustin%20Hurlbut/Documents/Uploads/WinkyAndBlinky.jpg
AccessedTime	8/13/2015 4:54:36 PM +0000
ModifiedTime	8/13/2015 4:54:36 PM +0000
ExpiryTime	9/8/2015 4:47:26 PM +0000
SyncTime	8/13/2015 4:54:36 PM +0000
AccessCount	1
Directory	C:\Users\Dustin Hurlbut\AppData\Local\Microsoft\Windows\History\History.IE5\
PartitionId	M
ContainerId	2
ResponseHeaders	00000000 79 00 00 00 75 00 00 00-31 53 50 53 A1 14 02 00 y...u...1SPS□...
Flags	0
SyncCount	1
Type	2097

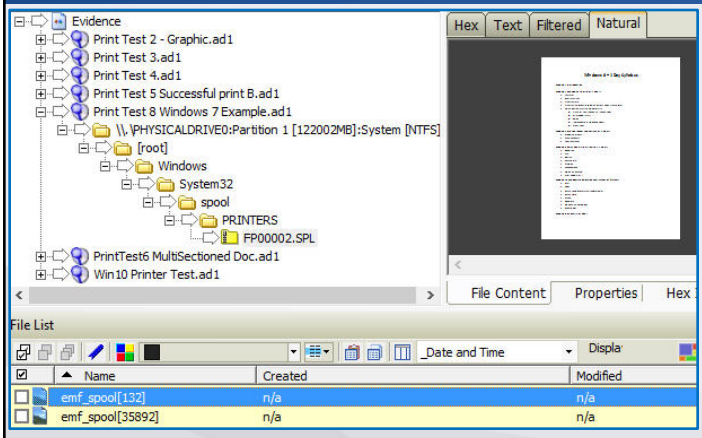
Name	Value
Url	:2015081320150814: Dustin Hurlbut@file:///C:/Users/Dustin%20Hurlbut/Documents/Uploads/WinkyAndBlinky.jpg
AccessedTime	8/13/2015 4:54:36 PM +0000
ModifiedTime	8/13/2015 12:54:36 PM +0000
ExpiryTime	9/8/2015 4:47:26 PM +0000
SyncTime	8/13/2015 4:54:36 PM +0000
AccessCount	1
Directory	C:\Users\Dustin Hurlbut\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012015081320150814\
PartitionId	M
ContainerId	60
ExemptionDelta	86400
Flags	4
SyncCount	0
Type	2097156

File Explorer – Tracking



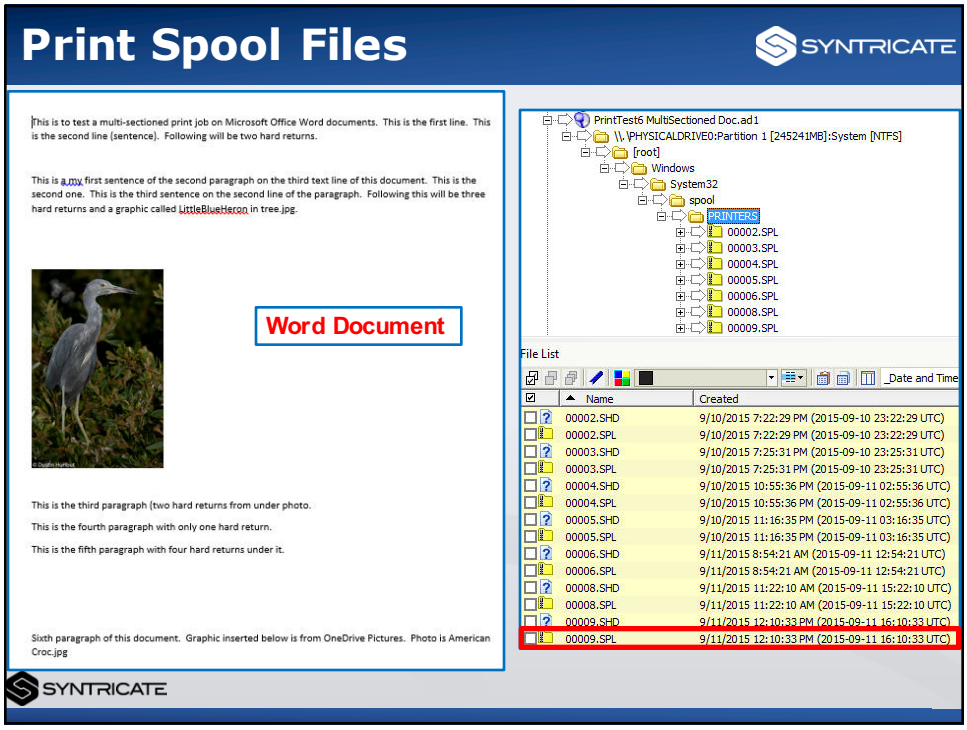
- Registry references to RecentDocs remains and allows checking on documents recently opened by the user
- Windows 10 now stores the last 20 rather than the last 10

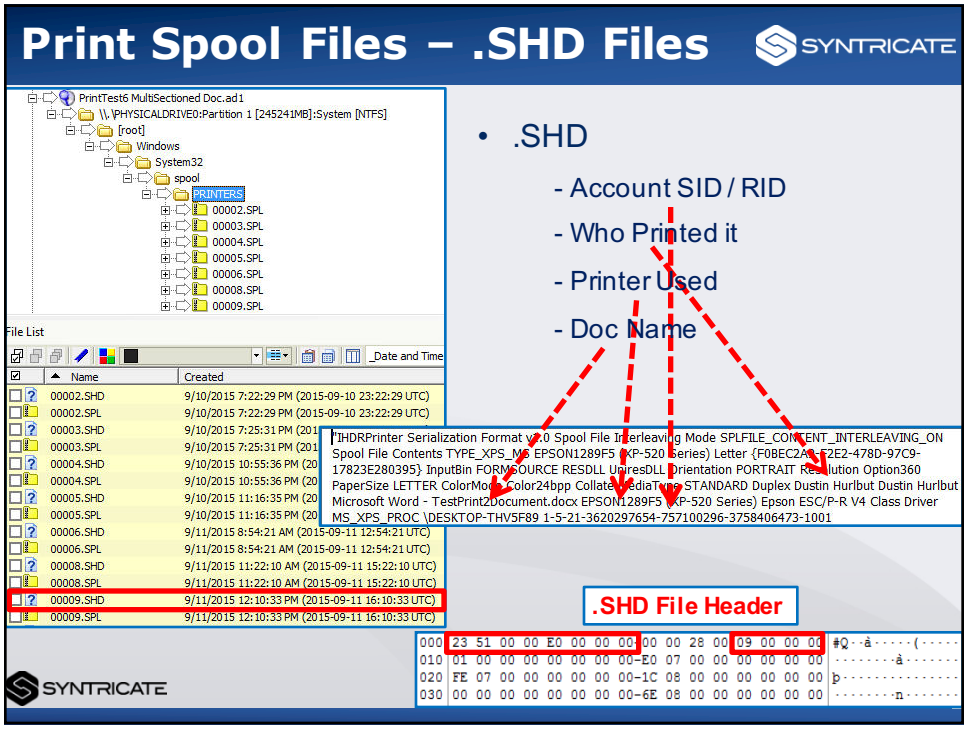
Print Spool Files - Previous



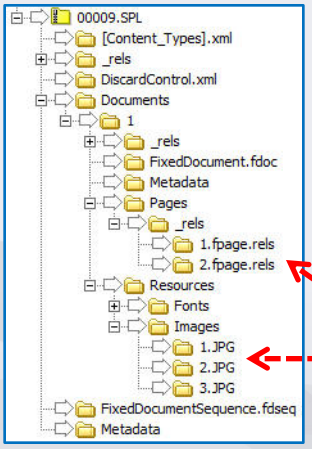
Pre Windows 8

- .SHD – Admin file tracks metadata about the print job
- .SPL – Archive file with an emf file embedded for each page of the print job


Print Spool Files
SYNTRICATE
This is to test a multi-sectioned print job on Microsoft Office Word documents. This is the first line. This is the second line (sentence). Following will be two hard returns.
This is a my first sentence of the second paragraph on the third text line of this document. This is the second one. This is the third sentence on the second line of the paragraph. Following this will be three hard returns and a graphic called LittleBlueHeron in tree.jpg.
This is the third paragraph (two hard returns from under photo.
This is the fourth paragraph with only one hard return.
This is the fifth paragraph with four hard returns under it.
Sixth paragraph of this document. Graphic inserted below is from OneDrive Pictures. Photo is American Croc.jpg
Word Document
PrintTest6 MultiSectioned Doc.ad1
\\.\PHYSICALDRIVE0:Partition 1 [245241MB]:System [NTFS]
[root]
Windows
System32
spool
PRINTERS
00002.SPL
00003.SPL
00004.SPL
00005.SPL
00006.SPL
00008.SPL
00009.SPL
File List
Name
Created
00002.SHD 9/10/2015 7:22:29 PM (2015-09-10 23:22:29 UTC)
00002.SPL 9/10/2015 7:22:29 PM (2015-09-10 23:22:29 UTC)
00003.SHD 9/10/2015 7:25:31 PM (2015-09-10 23:25:31 UTC)
00003.SPL 9/10/2015 7:25:31 PM (2015-09-10 23:25:31 UTC)
00004.SHD 9/10/2015 10:55:36 PM (2015-09-11 02:55:36 UTC)
00004.SPL 9/10/2015 10:55:36 PM (2015-09-11 02:55:36 UTC)
00005.SHD 9/10/2015 11:16:35 PM (2015-09-11 03:16:35 UTC)
00005.SPL 9/10/2015 11:16:35 PM (2015-09-11 03:16:35 UTC)
00006.SHD 9/11/2015 8:54:21 AM (2015-09-11 12:54:21 UTC)
00006.SPL 9/11/2015 8:54:21 AM (2015-09-11 12:54:21 UTC)
00008.SHD 9/11/2015 11:22:10 AM (2015-09-11 15:22:10 UTC)
00008.SPL 9/11/2015 11:22:10 AM (2015-09-11 15:22:10 UTC)
00009.SHD 9/11/2015 12:10:33 PM (2015-09-11 16:10:33 UTC)
00009.SPL 9/11/2015 12:10:33 PM (2015-09-11 16:10:33 UTC)
SYNTRICATE

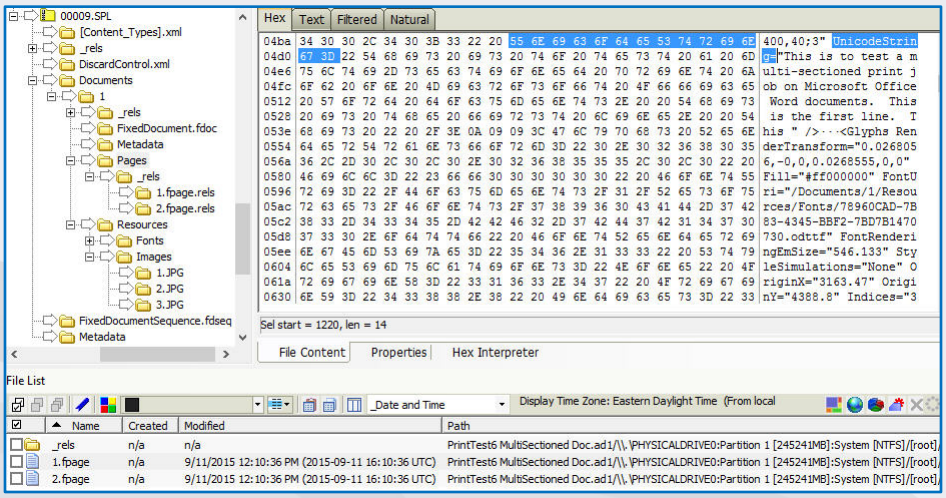

Print Spool Files – .SHD Files
SYNTRICATE
PrintTest6 MultiSectioned Doc.ad1
\\.\PHYSICALDRIVE0:Partition 1 [245241MB]:System [NTFS]
[root]
Windows
System32
spool
PRINTERS
00002.SPL
00003.SPL
00004.SPL
00005.SPL
00006.SPL
00008.SPL
00009.SPL
File List
Name
Created
00002.SHD 9/10/2015 7:22:29 PM (2015-09-10 23:22:29 UTC)
00002.SPL 9/10/2015 7:22:29 PM (2015-09-10 23:22:29 UTC)
00003.SHD 9/10/2015 7:25:31 PM (201
00003.SPL 9/10/2015 7:25:31 PM (201
00004.SHD 9/10/2015 10:55:36 PM (20
00004.SPL 9/10/2015 10:55:36 PM (20
00005.SHD 9/10/2015 11:16:35 PM (20
00005.SPL 9/10/2015 11:16:35 PM (20
00006.SHD 9/11/2015 8:54:21 AM (2015-09-11 12:54:21 UTC)
00006.SPL 9/11/2015 8:54:21 AM (2015-09-11 12:54:21 UTC)
00008.SHD 9/11/2015 11:22:10 AM (2015-09-11 15:22:10 UTC)
00008.SPL 9/11/2015 11:22:10 AM (2015-09-11 15:22:10 UTC)
00009.SHD 9/11/2015 12:10:33 PM (2015-09-11 16:10:33 UTC)
00009.SPL 9/11/2015 12:10:33 PM (2015-09-11 16:10:33 UTC)
• .SHD
- Account SID / RID
- Who Printed it
- Printer Used
- Doc Name
HDRPrinter Serialization Format v3.0 Spool File Interleaving Mode SPLFILE_CONTENT_INTERLEAVING_ON
Spool File Contents TYPE_XPS_MS EPSON1289F5 (XP-520 Series) Letter {F0BEC2A8-52E2-478D-97C9-17823E280395} InputBin FORMSOURCE RESDLL UnitresDLL Orientation PORTRAIT Resolution Option360
PaperSize LETTER ColorMode Color24bpp Collate MediaType STANDARD Duplex Dustin Hurlbut Dustin Hurlbut
Microsoft Word - TestPrint2Document.docx EPSON1289F5 (XP-520 Series) Epson ESC/P-R V4 Class Driver
MS_XPS_PROC \DESKTOP-THV5F89 1-5-21-3620297654-757100296-3758406473-1001
.SHD File Header
000 23 51 00 00 E0 00 00 00 00 00 28 00 09 00 00 00 #Q··à·····(·····
010 01 00 00 00 00 00 00 00-E0 07 00 00 00 00 00 00 ·····ä·····
020 FE 07 00 00 00 00 00 00-1C 08 00 00 00 00 00 00 þ·····
030 00 00 00 00 00 00 00 00-6E 08 00 00 00 00 00 00 ·····n·····
SYNTRICATE

Print Spool Files – Metadata



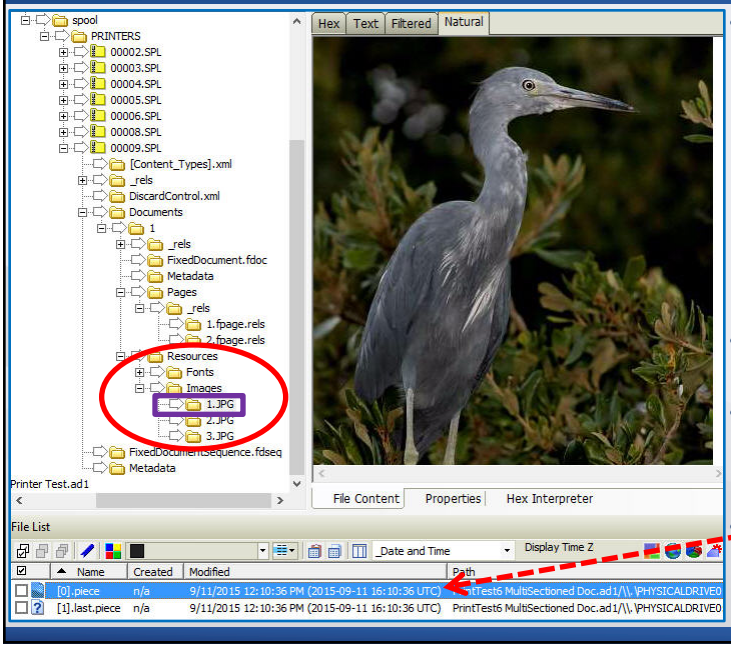
- Instead of .emf files stored in the .spl files, Microsoft is using what appears to be Office metadata structures
- The printed page is created from these archived files
- There are two locations of forensic interest:
  - Pages
  - Resources

Print Spool Files – Pages



- In the root of Pages, there is one #.fpage.rels for each page
- The text is stored line by line with header: UnicodeString=

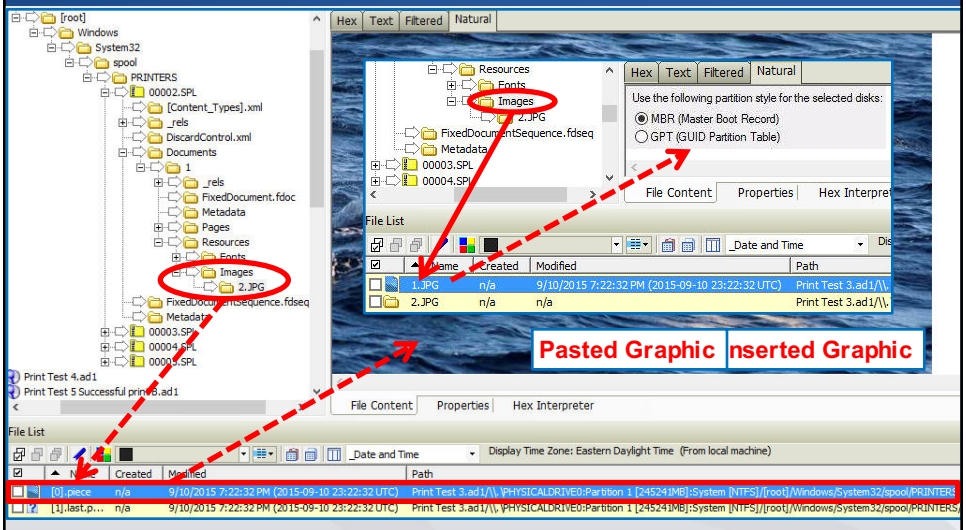
Print Spool Files – Resources



- Images inserted in the document using the Insert > Picture menu are stored under a sequential numbered folder
- One image per folder
- Graphic name will be:

  [0].piece
- Note the date / time is time doc was printed

Print Spool Files – Resources

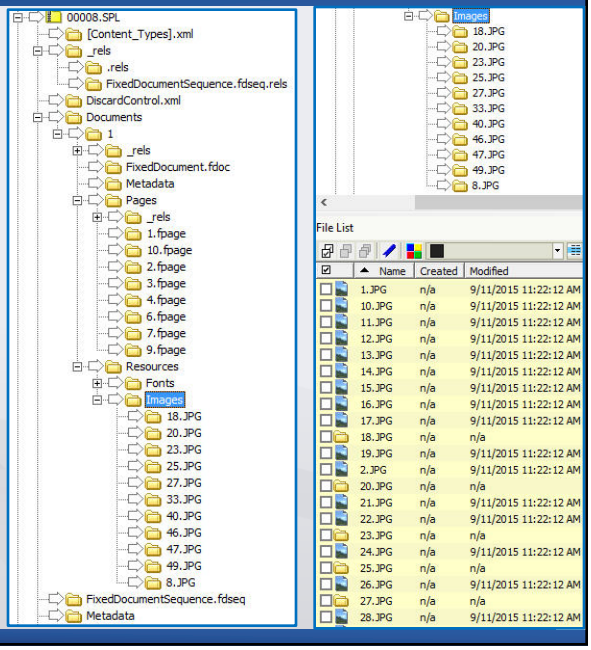


- Graphics pasted into the document are treated differently than ones that are added via the Insert > Picture menu (previous slide)

Print Spool Files – Other Docs

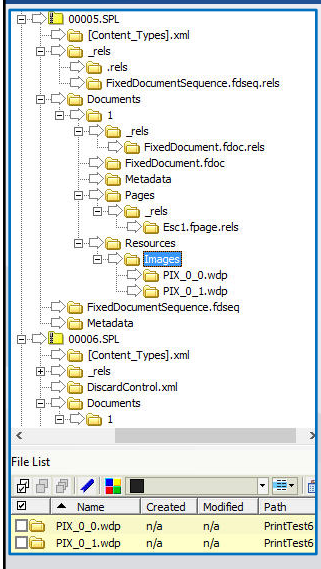
SYNTRICATE

- Large amounts of data can be processed for printing
- PDF file with 10 pages and over 50 graphics



Print Spool Files – Other Docs

SYNTRICATE



- Graphics files take different metadata
- No file name is present in .SHD
- No file type is noted
- A “Full page photo” reference is the indication of the printing of a graphic file such as a .jpg or .png

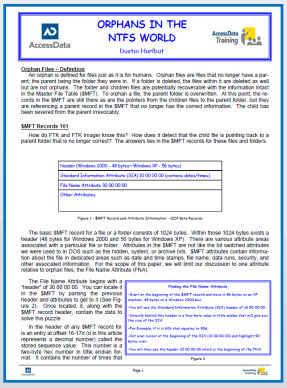
"IHDRPrinter Serialization Format v1.0 Spool File Interleaving Mode SPLFILE_CONTENT_INTERLEAVING_ON Spool File Contents TYPE_XPS_MS EPSON XP-520 Series Letter {F0BEC2A9-F2E2-478D-97C9-17823E280395} InputBin FORMSOURCE RESDLL UniresDLL Orientation LANDSCAPE_CC270 Resolution Option360 PaperSize LETTER ColorMode Color24bpp Collate MediaType STANDARD Duplex Dustin Hurlbut Dustin Hurlbut Full page photo EPSON XP-520 Series Epson ESC/P-R V4 Class Driver MS_XPS_PROC \DESKTOP-THV5F89 1-5-21-3620297654-757100296-3758406473-1001

Print Spool Files – Post Print

SYNTRICATE

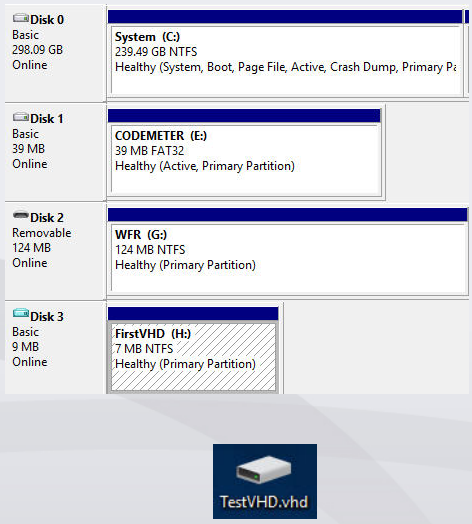
Name	Date Modified	Size
00007.SPL		
PP0d_mt8m0jpwntuu_ixzxy8ae.TMP	9/11/2015 2:52:57 PM	0
PP1s3l0npa0w0grwof6oubg47ce.TMP	9/11/2015 2:53:21 PM	0
PP283vxax4avvvl86zv5wtqybcb.TMP	9/11/2015 2:53:21 PM	0
PP3pagoe4op0e5fum9axndp63g.TMP	9/11/2015 2:53:21 PM	0
PP4j0jph1kuwh3rd64yj80jh70c.TMP	9/11/2015 2:53:21 PM	0
PP4ups_no7p0dkzd7i40v6g63_.TMP	9/11/2015 2:53:21 PM	0
PP5j07j0bc4itqt41smsinsx8md.TMP	9/11/2015 2:53:21 PM	0
PP7cuysctc7nfbwemcpu9bbmp5d.TMP	9/11/2015 2:53:21 PM	0
PP8jvmjgfhfnwm9f42dc9b0628d.TMP	9/11/2015 2:53:21 PM	0
PPas2ph0ht9_n3q4z_5jxo4ivvc.TMP	9/11/2015 2:53:21 PM	0
PPb9cxuwo4qov201xu46tmgnpyb.TMP	9/11/2015 2:53:21 PM	0
PPba0eoku143mx2_0c5lxuc41yb.TMP	9/11/2015 2:53:21 PM	0
PPctiqm03dikrjt1071bwm3ivdb.TMP	9/11/2015 2:53:21 PM	0
PPfmz4oil6cen9wotg0st_5uiwc.TMP	9/11/2015 2:53:21 PM	0
PPf_ezsj1iwpb_g71pyu24rvni.TMP	9/11/2015 2:53:21 PM	0
PPipt7d0tp5gon8r2qg52e74cy.TMP		
PPkxbw9ntrdrm92b0_zj8hj_0be.TMP	9/11/2015 2:53:21 PM	0
PPnm6vom8t0rnrk1crq6x980crc.TMP	9/11/2015 2:53:21 PM	0
PPokos245aw0ql410ghco03_pgc.TMP	9/11/2015 2:53:21 PM	0
PPoyqac3r55k21vokj4b8gfzq_b.TMP	9/11/2015 2:53:21 PM	0
PPp2lksgovvfl5fwubzc8h9bdmc.TMP	9/11/2015 2:53:21 PM	0
PPp5gispu8ycyzm0t5gy9enyj3c.TMP	9/11/2015 2:53:21 PM	0
PPp6m59pimms9hic_ej9rd3q6lc.TMP	9/11/2015 2:53:21 PM	0
PPq16ad12vk74nl5sysizf3e1lb.TMP	9/11/2015 2:53:21 PM	0
PPrxlv05qwku_ga5yo8uy837chc.TMP	9/11/2015 2:53:21 PM	0
PPrxlv05qwku_ga5yo8uy837chc.TMP		
PPRXLV~1.TMP		
PPscnewre78mih_851cog2av6pc.TMP	9/11/2015 2:53:21 PM	0
PPuda09rguoylwxudg2rhitzcl.TMP	9/11/2015 2:53:21 PM	0
PPustmbflmb37fl3jq71kqi_kjd.TMP	9/11/2015 2:53:21 PM	0
PPv_e6ze4zl2rro0pzpyqohe2kc.TMP	9/11/2015 2:53:21 PM	0
PPwa43i543lzwfh6kysmhe8xksc.TMP	9/11/2015 2:53:21 PM	0
PPx08etbkvogjjpg9pgalm2vb3b.TMP	9/11/2015 2:53:21 PM	0
PPxc9ec_6a8pfu_6nliu4bl930.TMP	9/11/2015 2:53:21 PM	0

- Results of a successful print on a .pdf file
- Note the zero byte status of each deleted file



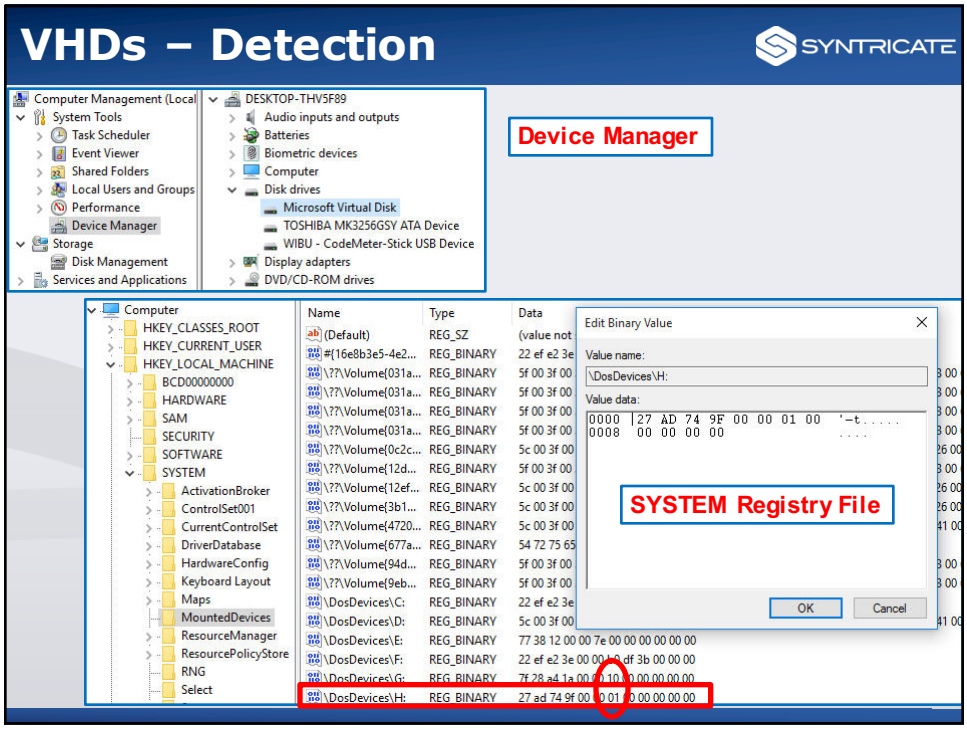
VHDs

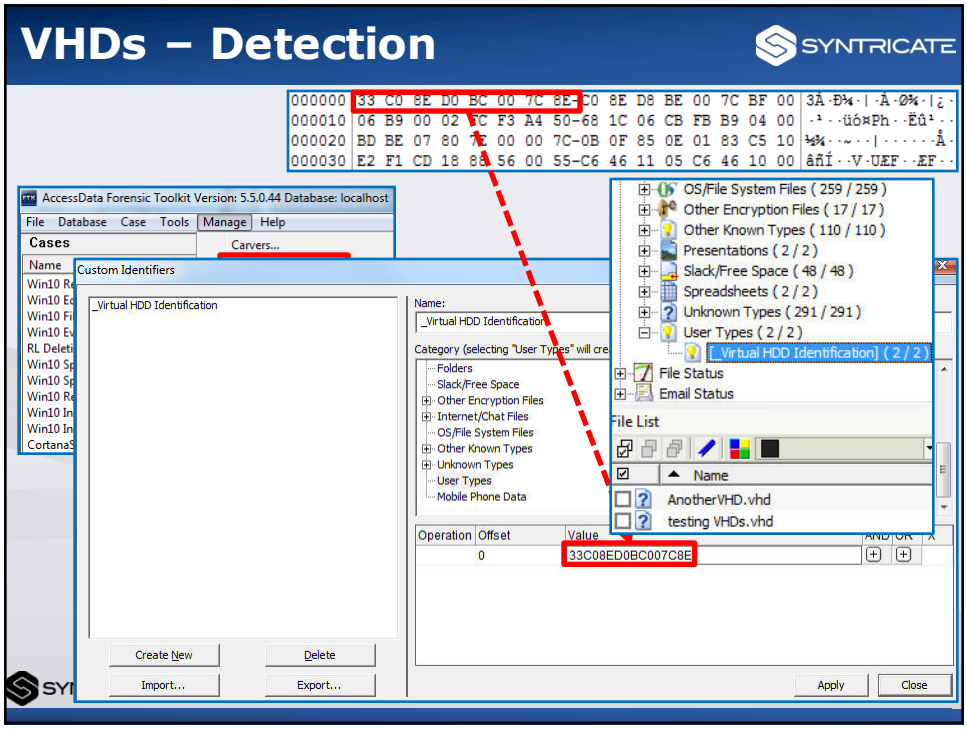
SYNTRICATE



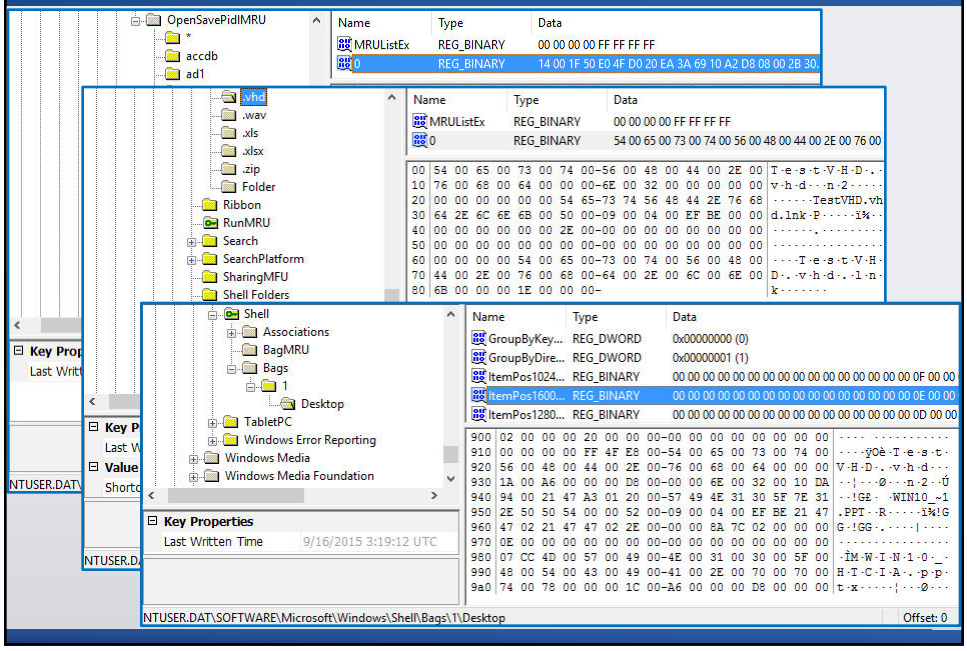
- VHD creation in Windows began with Windows 7
- They can be mounted with a double click or through Disk Management
- Artifacts are stored mainly in the registry and of course the VHD file in the file system
- VHDs can be encrypted with BitLocker

SYNTRICATE

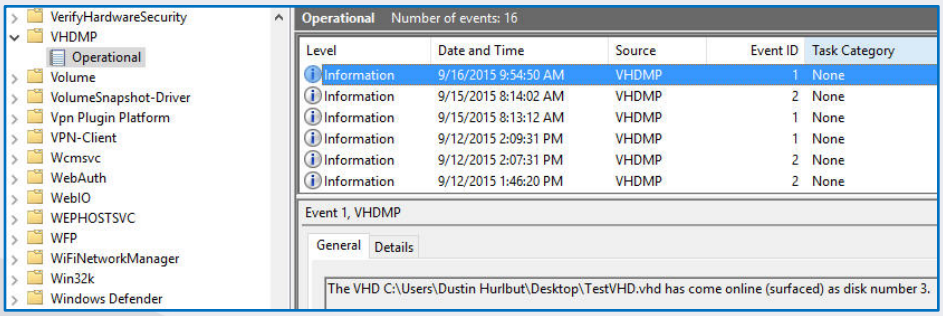

VHDs – Detection
SYNTRICATE
Device Manager
SYSTEM Registry File


VHDs – Detection
SYNTRICATE

VHDs – Registry Artifacts

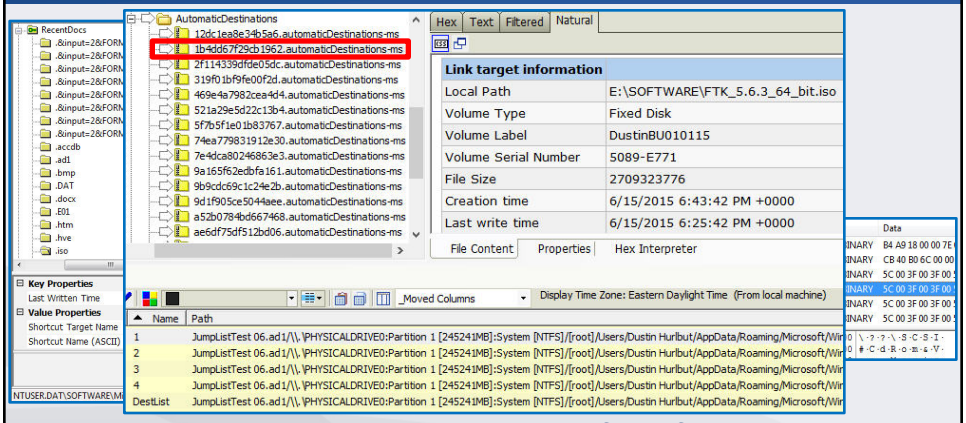


VHDs – Event Logs



- The System log file tracks the Virtual Disk Service
  - Opening a VHD will trip an Event ID #3 – "Virtual disk service started"
- VHDs have their own log file; VHDMP / Operational
  - Tracks opening with an Event ID #1 (tracks date/time, path and filename of .vhd and which disk number it occupied in the Disk Manager
  - Event ID #2 is the shutdown notification of the VHD

Mounting ISOs Directly



- Windows 10 permits direct mounting of .iso files
- Double click an ISO and it will be assigned a drive letter and be virtually accessible
- Don't forget the Jump List entries