

The image shows a grid of 12 computer monitors arranged in three rows of four. Each monitor displays a blue background with white text and small icons. The visible labels include:

- Automated eDiscovery
- Classified Data Spillage
- Criminal Investigation
- Compliance Auditing
- IP Theft
- Security Incident

The monitors are set against a dark blue background with a light blue gradient at the bottom. The Syntricate logo is in the top right corner and bottom left corner.

WIN10 – OS ARTIFACTS

Features

- 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



- 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

	Name	Date Modified	Size
	131e645fbfc71fe6.accountpicture-ms	8/26/2015 5:48:03 PM	37
	b49ee1ab2f3f3631.accountpicture-ms	8/26/2015 5:49:30 PM	37
0000	B2 90 00 00 AE 90 00 00-31 53 50 53 18 B0 6B 0B@...-1SPS-^...	
0010	25 27 44 4B 92 BA 79 33-AE B2 DD E7 15 0B 00 00	\$'DK-@y3@*Yç-...	
0020	04 00 00 00 00 42 00 00-00 1E 00 00 00 70 00 72B.....p r	
0030	00 6F 00 70 00 34 00 32-00 39 00 34 00 39 00 36	-o-p-4-2-9-4-9-6	
0040	00 37 00 32 00 39 00 35-00 00 00 00 00 DF 0A 00	-7-2-9-5-.....8-	
0050	00 FF D8 FF E0 00 10 4A-46 49 46 00 01 00 00	.ÿþà-JFIF.....	
0060	01 00 01 00 00 FF DB 00-84 00 05 05 05 05 05 05ÿû.....	
0070	06 06 06 06 08 09 08 09-08 0C 0B 0A 0A 0B 0C 12	



Supported Partition Types



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

Use the following partition style for the selected disks:

- MBR (Master Boot Record)
 GPT (GUID Partition Table)



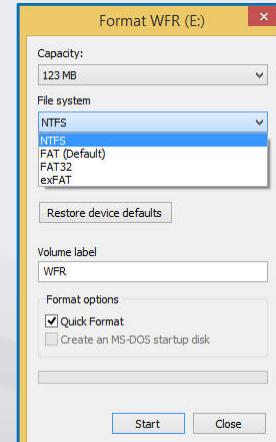
NTFS Version



- 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.

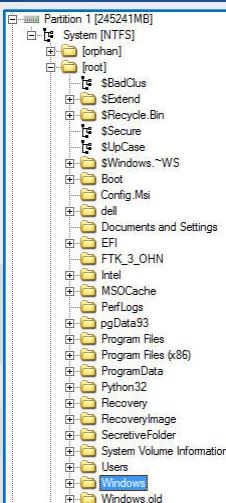
C:\WINDOWS\system32>fsutil fsinfo ntfsinfo c:
NTFS Volume Serial Number : 0x385894765894349a
NTFS Version : 3.1
LFS Version : 2.0
Number Sectors : 0x000000001defc7ff
Total Clusters : 0x0000000003bd8ff
Free Clusters : 0x0000000003b814c
Total Reserved : 0x00000000000010f0
Bytes Per Sector : 512
Bytes Per 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 : 0x0000000000000000
Mft2 Start Lcn : 0x0000000000000010
Mft Zone Start : 0x00000000001ef6ea0
Mft Zone End : 0x00000000001f030c0
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
```



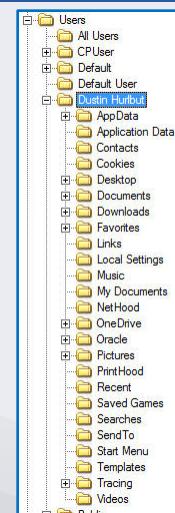
Resilient File System (ReFS) for Storage Pools



File Structure

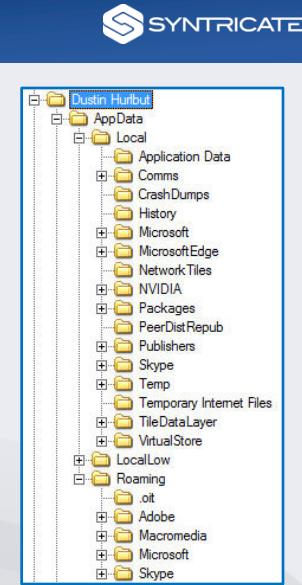


- The default root structure is similar to previous versions since Vista
- The user file system profile is also similar
- The now familiar UAC security from Vista is also present



File Structure

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



Recycle Bin

\$Recycle.Bin

Name	Size	Type	Date Modified
\$VWVX7Y.JPG	1	Regular File	5/13/2015 6:37:58 PM
SR267XDF.jpg	144	Regular File	7/31/2015 7:08:20 PM
SR267XDF.jpg.FileSlack	1	File Slack	
SR90QNTX.jpg	239	Regular File	4/11/2015 7:32:46 PM
SR90QNTX.jpg.FileSlack	2	File Slack	

\$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

```

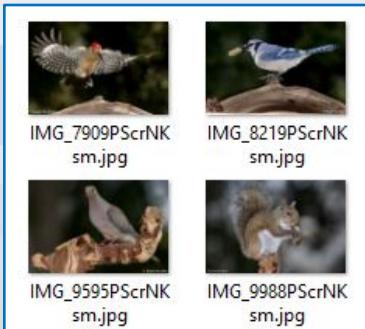
02 00 00 00 00 00 00-1F 3D 02 00 00 00 00 .....=.....
10 75 06 0C C5 CB D0 01-33 00 00 43 00 3A 00 -u-ÀED 3-C-:
5C 00 55 00 73 00 65 00-72 00 73 00 5C 00 53 00 \Users\S-
79 00 6E 00 74 00 72 00-5C 00 44 00 65 00 73 00 y-n-t-r\De-s-
6B 00 74 00 6F 00 70 00-5C 00 42 00 69 00 72 00 k-t-o-p\Bi-r-
64 00 73 00 5C 00 49 00-4D 00 47 00 5F 00 31 00 ut\d-s\I-M-G_1-
36 00 37 00 34 00 50 00-53 00 63 00 72 00 4E 00 6-7-4-P-S-c-r-N-
4B 00 73 00 73 00 6D 00-2E 00 6A 00 70 00 67 00 K-s-s-m..j-p-g.

```

Thumbnail Cache



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



ExplorerStartupLog.etl	6/30/2015 12:07 PM	ETL File	648 KB
iconcache_16	7/1/2015 4:26 PM	Data Base File	1,024 KB
iconcache_32	6/30/2015 12:07 PM	Data Base File	1,024 KB
iconcache_48	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_96	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_256	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_768	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_1280	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_1920	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_2560	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_custom_stream	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_exif	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_idx	6/30/2015 12:07 PM	Data Base File	8 KB
iconcache_sr	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_wide	6/30/2015 12:07 PM	Data Base File	1 KB
iconcache_wide_alternate	6/30/2015 12:07 PM	Data Base File	1 KB
thumbcache_16	6/30/2015 12:07 PM	Data Base File	1,024 KB
thumbcache_32	6/30/2015 12:07 PM	Data Base File	1,024 KB
thumbcache_48	6/30/2015 12:07 PM	Data Base File	1,024 KB
thumbcache_96	6/30/2015 12:07 PM	Data Base File	1,024 KB
thumbcache_256	6/30/2015 12:07 PM	Data Base File	1,024 KB
thumbcache_768	7/16/2015 10:58 AM	Data Base File	2,048 KB
thumbcache_1280	7/2/2015 4:19 PM	Data Base File	1,024 KB
thumbcache_1920	7/2/2015 4:51 PM	Data Base File	1,024 KB
thumbcache_2560	6/30/2015 12:07 PM	Data Base File	1 KB
thumbcache_custom_stream	6/30/2015 12:07 PM	Data Base File	1 KB
thumbcache_exif	7/16/2015 10:28 AM	Data Base File	1,024 KB
thumbcache_idx	7/16/2015 11:19 AM	Data Base File	29 KB
thumbcache_sr	6/30/2015 12:07 PM	Data Base File	1 KB
thumbcache_wide	6/30/2015 12:07 PM	Data Base File	1 KB
thumbcache_wide_alternate	6/30/2015 12:07 PM	Data Base File	1 KB

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

Thumbnail Cache



- 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 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 00 00	@-7-Y-zq
00030	E7 88 02 00 00 05 00 00-D0 02 00 00 00 00 00 00 00 00	ç.....D
00040	DD 53 66 F4 22 DA 86 24-04 6F 6B 4A 0C BC 25 81	ÝSfô"Ü-s-okJ-¾%
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 00 00	ÿþÿà-JFIF
00080	00 00 00 00 FF DB 00 43-00 04 03 03 04 03 04 07ÿÛ-C

Thumbnail Cache Temp Files

SYNTRICATE

This screenshot shows a file explorer window with a detailed view of a prefetch file. A specific folder path is highlighted:

```

Prefetch-ThumbCache01.ad1
  └─ Custom Content Image(Multi) [AD1]
    └─ Prefetch-ThumbCache01.ad1
      └─ AutomaticDestinations
        └─ 12dc1ea8e34b5a6.automaticDestinations-ms
          └─ 1b4dd6729b1962.automaticDestinations-ms
            └─ 2f11433edfd65dc.automaticDestinations-ms
              └─ 319f01b9f00f2d.automaticDestinations-ms
                └─ 469e4a7982ca4d4.automaticDestinations-ms
                  └─ 521a29e5d22c13b4.automaticDestinations-ms
                    └─ 5f7b5f1e01b83767.automaticDestinations-ms
                      └─ 7e4ea779831912e30.automaticDestinations-ms
                        └─ 9a165f62edbf6151.automaticDestinations-ms
                          └─ 9b9dc69c1c24e2b.automaticDestinations-ms
                            └─ 9d1f905ce504aee.automaticDestinations-ms
                              └─ a52b0784bd67468.automaticDestinations-ms
                                └─ ae6df75df512bd06.automaticDestinations-ms

```

The right pane displays the properties of a file named `DestList`:

Name	Path
1	JumpListTest 06.ad1\.\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\[root]\Users\Dustin Hurlbut\AppData\Roaming\Microsoft\Windows\JumpList\DestList
2	JumpListTest 06.ad1\.\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\[root]\Users\Dustin Hurlbut\AppData\Roaming\Microsoft\Windows\JumpList\DestList
3	JumpListTest 06.ad1\.\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\[root]\Users\Dustin Hurlbut\AppData\Roaming\Microsoft\Windows\JumpList\DestList
4	JumpListTest 06.ad1\.\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\[root]\Users\Dustin Hurlbut\AppData\Roaming\Microsoft\Windows\JumpList\DestList

Below the properties pane, the file content is shown in hex and ASCII format. The ASCII dump shows the file signature `JFIF` and other metadata.

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

Windows 10 Thumbs.db

SYNTRICATE

This screenshot shows the Windows 10 Thumbs.db database. It lists several image files with their names, sizes, creation dates, and modification dates.

Name	Size	Date created	Date modified
IMG_1971PScrNKsm.jpg	102 KB	10/31/2015 9:51 AM	4/25/2015 7:08 PM
IMG_2004PScrNKsm.jpg	92 KB	10/31/2015 9:51 AM	4/25/2015 7:20 PM
IMG_5436PScrNKsm.jpg	256 KB	10/31/2015 9:51 AM	4/25/2015 2:06 PM
IMG_5514PScrNKsm.jpg	140 KB	10/31/2015 9:51 AM	4/25/2015 2:31 PM
IMG_5796PScrNKsm.jpg	143 KB	10/31/2015 9:51 AM	4/25/2015 2:52 PM
IMG_5889PScrNKsm.jpg	159 KB	10/31/2015 9:51 AM	4/25/2015 3:12 PM
IMG_5934PScrNKsm.jpg	80 KB	10/31/2015 9:51 AM	4/25/2015 3:28 PM
IMG_5966PScrNKsm.jpg	116 KB	10/31/2015 9:51 AM	4/25/2015 3:35 PM

To the right of the table is a preview image of a bird's head.

The bottom right corner shows a hex dump of the Thumbs.db file, which includes the file signature `JFIF`.

- 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

This PC > Local Disk (T)

Search Local Disk (T)

Thumbnails

File Content

File Content Properties Hex Interpreter

File List

```
Path: thumbdrive08.ad1\|\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\root\Users\DustinHurlbut\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db\Carved [1017928].jpeg
      thumbdrive08.ad1\|\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\root\Users\DustinHurlbut\AppData\Local\Microsoft\Windows\Explorer\thumbcache_48.db\Carved [102450].bmp
      thumbdrive08.ad1\|\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\root\Users\DustinHurlbut\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db\Carved [1027146].jpeg
      thumbdrive08.ad1\|\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\root\Users\DustinHurlbut\AppData\Local\Microsoft\Windows\Explorer\thumbcache_16.db\Carved [10394].bmp
```

Loaded: 401 Filtered: 401 Total: 427 Highlighted: 1 Checked: 401 Total LSize: 9440 KB Show Tooltip

Prefetch Files – Compression

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

File Name	Last Modified	File Size	File Content
ReadyBoot	10/25/2015 1:42:00 PM	0000	0000 4D 41 4D 04 B2 6B 00 00-A4 B8 B6 BA B9 B8 AB AB MAM- ^k -s, [¶] ..<>
ACCESSDATA FTK IMAGER.EXE-3ADF8A94.pf	8/3/2015 8:51:27 PM	0010	0010 AA C7 BA AB A9 B7 AB BA-C8 B7 AA AB C9 07 9B B8 ^C<>@-<>É- ^k -.
ACCESSDATA FTK SUITE (64-BIT)-1D7DFE3B.pf	8/27/2015 10:26:25 PM	0020	0020 98 97 A9 9A A9 B7 B0 AB-89 87 89 99 99 A7 98 99 .-@.-@-.<>...-S-.
ACCESSDATA PASSWORD RECOVERY -08622FF1.pf	8/27/2015 10:58:56 PM	0030	0030 C8 87 98 9A B8 07 CB 90-B9 B7 CC B0 09 B7 BB B0 É-..-E- ^k -.->.
ACORD32.EXE-62938E59.pf	8/3/2015 8:44:17 PM		B9-B9 08 CB BA A9 08 0B BB ÉCÉ- ^k -S- [¶] ..-É- [¶] -..>
AgAppLaunch.db	10/16/2015 4:32:10 PM		BB-B9 07 0B BC B9 B7 CA CB ^-É- ^k -..-A- [¶] -É-.
ACCESSDATA REGISTRY VIEWER.EX-0259034.Apf	8/27/2015 11:30:05 PM		CC-B9 B8 CB 0C B9 B8 CB AA .C- ^k ->I- ^k ,É-..É-.
AgCx_SC1.db	10/29/2015 1:13:51 PM		BC-0A C8 BA BB C9 C8 BB BC ÉÉAÍÉ,É- ^k -E- [¶] -É-É-.
AgCx_SC1.db.trx	10/29/2015 1:12:50 PM		9A-0C 00 00 00 00 00 00 00 É,- [¶] -.
AgCx_SC2.db	10/29/2015 1:14:55 PM		00-79 0C 0B 00 00 00 00 C0y-.....À
			C0-97 AA C7 00 00 0C 00 B0 -SÀ-..-À- [¶] -.
			A0-97 9C A9 00 9B 00 9B 90 !-..-<-..-.
			80-A7 A8 77 80 AC BC BB B0 ..-i-..-S- [¶] -.
			80-87 A9 98 CC BC CO BO 8C ..-w-..-@-P-À-.
			80-90 B9 A9 0B B0 0C 00 A0 E- [¶] -À-..-@-.
			0100 00 00 00 00 00 00 00 ..-..-À-..-.
			0110 0F B2 AA BC FA 24 74 50-14 EA E9 A4 EB D8 4B 2D ..-#ùstP-ééhëòK-

Prefetch Files-Decompression

SYNTRICATE

0000	4D 41 4D 04 B2 6B 00 00-A4 B8 B6 BA B9 B8 AB AB	MAM..K..H..I..<<
0010	AA C7 BA AB A9 B7 AB BA-C8 B7 AA AB C9 07 9B B5	*C*@-<*E-<*E..
0020	98 97 A9 9A A9 B7 B0 AB-B9 87 89 99 99 A7 98 99	..@. @. "....\$..
0030	C8 87 98 9A B8 07 C8 90-B9 B7 CC B0 09 B7 BB B6	..@.., .E.., ..\$..>>
0040	C9 C7 CB BA B9 A7 BA-B9 08 CB BA A9 08 08 BE	EEC*!S*11..E*..>>
0050	AA 07 CA CC BA B7 CA BB-B9 07 08 BC B9 B7 CA CB	*E*..E*.., ..I.., E.., E*
0060	09 C7 0B BC B9 B7 BB CC-B9 B8 CB 0C B9 B8 CB AA	.., ..I.., E.., E*
0070	C9 C8 C0 CC C9 B8 BB BC-0A C8	Compressed
0080	0000 1E 00 00 00 53 43 43 41-11 00 00 00 00 B2 6B 00 00	...SCCA...-k..
0090	0A 00 0C 00 00 00 00 00-79 0C	A-C-C-E-S-S-D-A.
0000	41 00 43 00 43 00 45 00-53 00 53 00 44 00 41 00	T-A..F-T-K..I..
0010	54 00 41 00 20 00 46 00-54 00 4B 00 20 00 49 00	..T-A..
0020	00 00 00 00 30 01 00 00-37 00 00 00 10 08 00 00	F-T-K..I..
0030	4D 00 41 00 47 00 45 00-52 00 2E 00 45 00 58 00	M-A-G-E-R..E-X..
0040	45 00 00 00 00 00 00 00-00 00 00 00 94 8A DF 3A	E-----B:
0050	00 00 00 00 30 01 00 00-37 00 00 00 10 08 00 00	..O..7..
0060	58 07 00 00 D0 42 00 00-2E 1E 00 00 00 61 00 00 X---DB..,....a..	X---DB..,....a..
0070	01 00 00 00 B2 0A 00 00-OF 00 00 00 01 00 00 00	..a..
0080	D8 42 84 24 2E CE D0 01-00 00 00 00 00 00 00 00 00	OB \$.Id.....
0090	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00
00A0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00
00B0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00
00C0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00
00D0	01 00 00 00 01 00 00 00-03 00 00 00 00 00 00 00 00
00E0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00

Decompressed

- Decompression using Python script
- Script written by Francesco Picasso

Prefetch Files – Offsets

SYNTRICATE

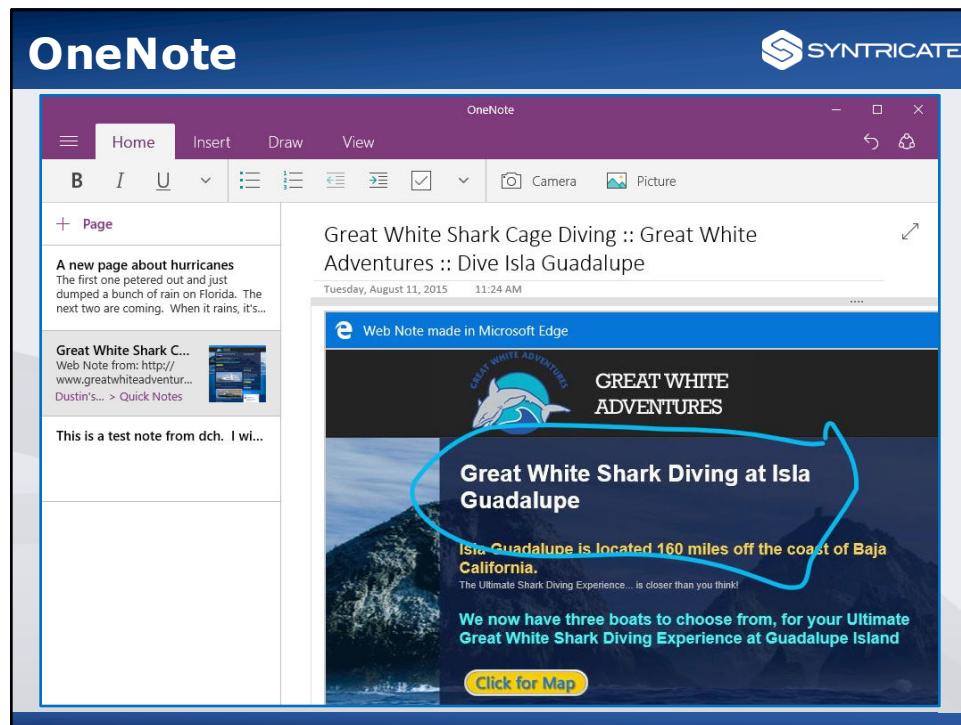
0000	1E 00 00 00 53 43 43 41-11 00 00 00 70 5E 00 00	...SCCA...-p..	
0010	48 00 45 00 41 00 44 00-45 00 52 00 20 00 45 00	H-E-A-D-E-R..E..	
0020	58 00 54 00 52 00 41 00-43 00 54 00 2E 00 45 00	X-T-R-A-C-T..E..	
0030	58 00 45 00 00 00 00-00 00 00 00 00 00 00 00 00	X-E..	
0040	00 00 00 00 00 00 00-00 00 00 00 00 57 19 7E C50..	
0050	00 00 00 00 30 01 00 00-2D 00 00 00 00 00 00 00 000..	
0060	CD 06 00 00 38 3D 00 00-2E 18 00 68 55 00 00	i...8=..,..hU..	
0070	01 00 00 00 08 09 00 00-0C 00 00 01 00 00 00	
0080	A4 F9 C9 43 75 12 D1 01	First use d/t starts at offset 128	
0090	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
00A0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
00B0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
00C0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
00D0	01 00 00 00 01 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00E0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
00F0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0100	48 00 45 00 41 00 44 00-45 00 52 00 20 00 45 00	H-E-A-D-E-R..E..	
0110	58 00 54 00 52 00 41 00-43 00 54 00 2E 00 45 00	X-T-R-A-C-T..E..	
0120	58 00 45 00 00 00 00-00 00 00 00 00 00 00 00 00	X-E..	
0130	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00W..Ä	
0140	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 000..-D..	
0150	01 00 00 00 08 09 00 00-0C 00 00 01 00 00 000..-D..	
0160	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00D..-P..-U..	
0170	01 00 00 00 08 09 00 00-0C 00 00 01 00 00 00D..-P..-U..	
0180	A5 F8 D4 D3 75 12 D1 01	Second use moves over 8 bytes	
0190	A4 F9 C9 43 75 12 D1 01	
01A0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
01B0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
01C0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
01D0	02 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
01E0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
01F0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0200	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0210	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0220	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0230	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0240	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0250	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0260	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0270	01 00 00 00 08 09 00 00-0C 00 00 01 00 00 00	
0280	A5 F8 D4 D3 75 12 D1 01	Third use moves over 8 more bytes	
0290	A4 F9 C9 43 75 12 D1 01	
02A0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
02B0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
02C0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
02D0	02 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
02E0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
02F0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0300	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0310	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0320	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0330	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0340	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0350	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0360	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0370	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
0380	05 F4 75 5C 76 12 D1 01-A5 F8 D4 D3 75 12 D1 01	Note the count changes	
0390	A4 F9 C9 43 75 12 D1 01	
03A0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
03B0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
03C0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
03D0	03 00 00 00 01 00 00 00-03 00 00 00 00 00 00 00	

First use d/t starts at offset 128

Second use moves over 8 bytes

Third use moves over 8 more bytes

Note the count changes



OneNote BIN Files

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

The screenshot shows a file explorer window displaying the file structure of a OneNote bin file. The path is C:\Users\<username>\AppData\Local\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\LocalState\Local\OneNote\16.0\cache. The right pane shows the contents of one of these files, which contains a large amount of salting text used for tracking changes in the file system.

Name	Created	Modified	Accessed	Path
tmp	8/11/2015 11:25:15 AM (2015-08-11 15:25:15 UTC)	9/17/2015 8:11:14 AM (2015-09-17 12:11:14 UTC)	9/17/2015 8:11:14 AM (2015-09-17 12:11:14 UTC)	OneNoteTest02.ad1 \PHYSICALDRIVE0\Pa
header	8/11/2015 11:25:15 AM (2015-08-11 15:25:15 UTC)	9/17/2015 8:12:11 AM (2015-09-17 12:12:11 UTC)	8/11/2015 11:25:15 AM (2015-08-11 15:25:15 UTC)	OneNoteTest02.ad1 \PHYSICALDRIVE0\Pa
0000000c.bn	8/11/2015 12:10:26 PM (2015-08-11 16:10:26 UTC)	9/17/2015 12:11:38 PM (2015-08-11 16:11:38 UTC)	8/11/2015 12:10:26 PM (2015-08-11 16:10:26 UTC)	OneNoteTest02.ad1 \PHYSICALDRIVE0\Pa
00000009.bn	8/11/2015 12:07:48 PM (2015-08-11 16:07:48 UTC)	8/11/2015 12:07:48 PM (2015-08-11 16:07:48 UTC)	8/11/2015 12:07:48 PM (2015-08-11 16:07:48 UTC)	OneNoteTest02.ad1 \PHYSICALDRIVE0\Pa
00000008.bn	8/11/2015 12:07:47 PM (2015-08-11 16:07:47 UTC)	8/11/2015 12:07:47 PM (2015-08-11 16:07:47 UTC)	8/11/2015 12:07:47 PM (2015-08-11 16:07:47 UTC)	OneNoteTest02.ad1 \PHYSICALDRIVE0\Pa

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

OneNote – ShareMFU

SYNTRICATE

- This MRU is tracking shares from OneNote

Name	Type	Data
MRUListEx	REG_BINARY	00 00 00 00 01 00 00 02 00 00 03 00 00 FF FF FF FF
MRUListEx	REG_BINARY	AA 04 00 A6 04 00 31 53 50 53 05 D5 CD D5 9C 2E 1B
MRU1	REG_BINARY	CE 04 00 CA 04 00 31 53 50 53 05 D5 CD D5 9C 2E 1B
MRU2	REG_BINARY	CA 04 00 C6 04 00 31 53 50 53 05 D5 CD D5 9C 2E 1B
MRU3	REG_BINARY	B6 04 00 B2 04 00 31 53 50 53 05 D5 CD D5 9C 2E 1B

OneNote MRUListEx anomaly

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

OneNote – Settings.dat

SYNTRICATE

- Settings.dat identity information

Name	Type	Data
dP	0x5F5E105	01 00 00 00 EF C5 92 DF 49 D4 D0 01
ProviderId	0x5F5E10C	61 00 65 00 38 00 39 00 39 00 33 00 37 00 64 00 33 00 63 0
SigninName	0x5F5E10C	00 00 EF C5 92 DF 49 D4 D0 01
EmailAddress	0x5F5E10C	64 00 75 00 73 00 74 00 69 00 6E 00 73 00 79 00 6E 00 74 0
FirstName	0x5F5E10C	44 00 75 00 73 00 74 00 69 00 6E 00 00 00 A0 7D 2D E0 49
LastName	0x5F5E10C	48 00 75 00 72 00 6C 00 62 00 75 00 74 00 00 A0 7D 2D E0 49
FriendlyName	0x5F5E10C	44 00 75 00 73 00 74 00 69 00 6E 00 20 00 48 00 75 00 72 0
Initials	0x5F5E10C	44 00 48 00 00 A0 7D 2D E0 49 D4 D0 01
Picture	0x5F5E10C	00 00 A0 7D 2D E0 49 D4 D0 01
ProfileUrl	0x5F5E10C	00 00 A0 7D 2D E0 49 D4 D0 01
Persisted	0x5F5E105	01 00 00 00 98 6C 98 DF 49 D4 D0 01

ae89957d3cd5ce3_Lived

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

SYNTRICATE

File Explorer – Tracking

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

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

Link Files and Jump Lists

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

Relative Path	..\..\..\..\..\Desktop\SaveAsTestDTtoOD.docx
Working directory	C:\Users\Dustin Hurlbut\Desktop

Optional fields

File Content	Properties	Hex Interpreter
--------------	------------	-----------------

File List

Name	Created	Modified	Accessed
SAR05AD-Syn.png.lnk	8/4/2015 8:57:12 PM (2015-08-05 00:57:12 UTC)	8/4/2015 8:57:12 PM (2015-08-05 00:57:12 UTC)	8/4/2015 8:57:12 PM (2015-08-05 00:57:12 UTC)
SAR06AD-Syn.png.lnk	8/4/2015 8:57:47 PM (2015-08-05 00:57:47 UTC)	8/4/2015 8:57:47 PM (2015-08-05 00:57:47 UTC)	8/4/2015 8:57:47 PM (2015-08-05 00:57:47 UTC)
SAR07 ms win10.png.lnk	8/4/2015 8:59:22 PM (2015-08-05 00:59:22 UTC)	8/4/2015 8:59:22 PM (2015-08-05 00:59:22 UTC)	8/4/2015 8:59:22 PM (2015-08-05 00:59:22 UTC)
sar08 where is croatia VOICE.png.lnk	8/4/2015 9:02:04 PM (2015-08-05 01:02:04 UTC)	8/4/2015 9:02:04 PM (2015-08-05 01:02:04 UTC)	8/4/2015 9:02:04 PM (2015-08-05 01:02:04 UTC)
sar09 what is technico security VOICE.png.lnk	8/4/2015 9:03:08 PM (2015-08-05 01:03:08 UTC)	8/4/2015 9:03:08 PM (2015-08-05 01:03:08 UTC)	8/4/2015 9:03:08 PM (2015-08-05 01:03:08 UTC)
SaveAsTestDTtoOD.docx.lnk	8/25/2015 11:59:15 AM (2015-08-25 15:59:15 UTC)	9/10/2015 8:52:54 AM (2015-09-11 12:52:54 UTC)	9/11/2015 8:52:54 AM (2015-09-11 12:52:54 UTC)
ScreenCaptureTest.jpg.lnk	9/13/2015 8:25:42 AM (2015-09-13 12:25:42 UTC)	9/13/2015 8:25:42 AM (2015-09-13 12:25:42 UTC)	9/13/2015 8:25:42 AM (2015-09-13 12:25:42 UTC)
Search test (2).lnk	8/8/2015 4:31:53 PM (2015-08-08 20:31:53 UTC)	8/8/2015 8:18:44 PM (2015-08-09 00:18:44 UTC)	8/8/2015 8:18:44 PM (2015-08-09 00:18:44 UTC)
Search test (3).lnk	8/8/2015 8:34:58 PM (2015-08-09 00:34:58 UTC)	8/9/2015 10:56:09 AM (2015-08-09 14:56:09 UTC)	8/9/2015 10:56:09 AM (2015-08-09 14:56:09 UTC)
Search test.lnk	8/8/2015 9:18:57 AM (2015-08-08 13:18:57 UTC)	8/8/2015 4:31:05 PM (2015-08-08 20:31:05 UTC)	8/8/2015 4:31:05 PM (2015-08-08 20:31:05 UTC)

Link Files – Tracking



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

Link File Basics



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	DRIV	Hex Value Interpreter	Description
0x 00000000	DRIV	Type	't be determined
0x 00000001	DRIV	signed integer	is invalid
0x 00000002	DRIV	unsigned integer	1-8 175,509 edia
0x 00000003	DRIVE		HDD
0x 00000004	DRIVE		work drive
0x 00000005	DRIVE		Offset 44-51 ve
0x 00000006	DRIVE_RAMDISK		RAM disk
Volume Type Designators			
1a0 44 00 65 00 73 00 6B 00-74 00 6F 00 70 00 5C 00	1b0 53 00 61 00 76 00 65 00-41 00 73 00 54 00 65 00	1c0 73 00 74 00 44 00 54 00-74 00 6F 00 4F 00 44 00	1d0 2E 00 64 00 6F 00 63 00-78 00 1F 00 43 00 3A 00
1e0 5C 00 55 00 73 00 65 00-72 00 73 00 5C 00 44 00	1f0 75 00 73 00 74 00 69 00-6E 00 20 00 48 00 75 00	200 72 00 6C 00 62 00 75 00-74 00 5C 00 44 00 65 00	210 73 00 6B 00 74 00 6F 00-70 00 60 00 00 00 03 00

Distributed Link Tracking



```
C:\>fsutil objectid query ObjID.txt
Object ID : 5cd22d31a89ae5119bfaa4badbba220f
BirthVolume ID : 0a874aede0ae614e93631190fd99c7e5
BirthObjectId ID : 5cd22d31a89ae5119bfaa4badbba220f
Domain ID : 0000000000000000000000000000000000000000

C:\>
```

Current Location

- 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



SMFT	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-	Iyh-		
00a49010	2E	00	01	38	00	01	00	-60	E1	00	00	00	04	00	00	00	..-B-			
00a49020	00	00	00	00	00	00	00	-06	00	00	24	29	00	00	00	00		-\$		
00a49030	03	00	00	00	00	00	00	-10	00	00	60	00	00	00	00	00	H-			
00a49040	00	00	00	00	00	00	00	-48	00	00	18	00	00	00	00	00				
00a49050	52	78	30	B2	93	41	D1	-11	28	E9	A9	B2	93	41	D1	01	Rxo*-AN	(64*-AN		
00a49060	28	E9	AD	BD	93	41	D1	-01	52	78	B2	93	41	D1	01	(64*-AN	Rxo*-AN			
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		-S-		
00a49090	38	B9	59	E6	00	00	00	-00	30	00	00	70	00	00	00	00	B*Y*	0-p		
00a490A0	00	00	00	00	00	00	04	-00	54	00	00	18	00	01	00	00		I-		
00a490B0	42	18	00	00	00	79	00	-52	78	30	B2	93	41	D1	01	B-	YRxo*-AN			
00a490C0	52	78	30	B2	93	41	D1	-01	52	78	30	B2	93	41	D1	01	Rxo*-AN	Rxo*-AN		
00a490D0	52	78	30	B2	93	41	D1	-01	00	00	00	00	00	00	00	00	Rxo*-AN			
00a490E0	00	00	00	00	00	00	00	-00	20	00	00	00	00	00	00	00				
00a490F0	09	03	47	06	00	6A	00	-49	00	44	00	2E	00	74	00	-O-B-j-I-D-t				
00a49100	78	70	00	00	00	00	-00	40	00	00	28	00	00	00	00	x-t-	0-(
00a49110	00	00	00	00	00	00	05	-10	00	00	18	00	00	00	00					
00a49120	5C	02	2D	31	A8	9A	E5	-11	9B	FA	A4	BD	RA	22	0F	Ö-1	å	üñU"		
00a49130	80	00	00	28	00	00	00	-00	18	00	00	01	00	00	00					
00a49140	0C	00	00	18	00	00	00	-04	65	66	6E	20	57	6F	01		Hellin Wo			
00a49150	72	6C	64	21	00	00	00	-FF	FF	FE	FF	82	79	47	11	r1d1	VVV-V			

- 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

1

ObjId.txt.link	1 - Regular File	12/28/2015 15:18:07 PM
1a0 00 50 00 2B 00 00 5C-00 4C 00 69 00 60 6B	..\\..\\L-1-n-k	
1b0 00 50 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	..\\Link-T-e-s-t-.X-	
1e0 00 73 00 74 00 60 00 00-03 00 00 00 58 00 00 00	s-t-.X-\\	
1f0 00 00 00 00 64 65 73-6B 4E 70 7D 74 68 76	..\\desktop-chv	
200 35 66 38 39 00 00 04 67 4A-ED E0 AE 61 4E 93 63	f589 ..\\JaimeL	
210 90 FD 99 CT 15 EC 02 D2-2D-31 A5 9E 01 11 9B FA	..\\..\\JaimeL	
220 BA DB BA 22 00 08 07 4A-ED E0 AE 61 4E 93 63	..\\..\\JaimeL	
230 90 FD 99 CT 15 EC 02 D2-2D-31 A5 9E 01 11 9B FA	..\\..\\JaimeL	
240 BA DB BA 22 00 08 07 45 00-00-04 09 00 00 3A 09 00	E ..\\..\\JaimeL	
250 00 31 53 50 B3 16 64-AD ED 70 48 A7 48 40 15 08FB-#m-p@SSE	..\\..\\JaimeL	
260 2E A4 3D 78 8C 1D 00-00-04 68 00 00 00 00 48 00	..\\..\\JaimeL	
270 00 00 22 EF E2 3E 00 00-00-00 00 00 00 10 00 00 00	..\\..\\JaimeL	
280 00 00 00 00 00 00-00-00 00 00 00 00 00 00 00 00	..\\..\\JaimeL	

Link File Basics – Back End



	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\0-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 03 00 00 A0 58 00 00	..\..\..\X..	
1f0	00 00 00 00 00 64 65 73-6B 74 6F 70 71 74 68 76	..\..\..\desktop-thv	
200	35 66 38 39 00 0A 87 4A-ED E0 AE 61 4E 93 63 11	5f89..JiàoaN.c.	
210	90 FD 99 C7 E5 5C D2 2D-31 A8 9A E5 11 9B FA A4	ÿ Çà\0-1"åú	
220	BA DB BA 22 0F 0A 87 4A-ED E0 AE 61 4E 93 63 11	ºÛº"..\JiàoaN.c.	
230	90 FD 99 C7 E5 5C D2 2D-31 A8 9A E5 11 9B FA A4	ÿ Çà\0-1"åú	
240	BA DB BA 22 0F 45 00 00-00 09 00 00 A0 39 00 00	1SPS+..mD-pHSnE	
250	00 31 53 50 53 B1 16 6D-44 AD 8D 70 48 A7 40 40	..H..x..H..	
260	2E A4 3D 78 8C 1D 00 00-00 68 00 00 00 00 48 00	.H=x..H..	
270	00 00 22 EF E2 3E 00 00-00 00 00 00 10 00 00 00	..iâ>.....	
280	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	

- 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..JiàoaN.c.
210	90 FD 99 C7 E5 5C D2 2D-31 A8 9A E5 11 9B FA A4	ÿ Çà\0-1"åú
220	BA DB BA 22 0F 0A 87 4A-ED E0 AE 61 4E 93 63 11	ºÛº"..\JiàoaN.c.
230	90 FD 99 C7 E5 5C D2 2D-31 A8 9A E5 11 9B FA A4	ÿ Çà\0-1"åú
240	BA DB BA 22 0F 45 00 00-00 09 00 00 A0 39 00 00	ºÛº"E.....9..

Link File Basics – Moved File



	ObjID.txt.lnk	1 Regular File	12/28/2015 5:29:16 PM
0e0	00 01 00 00 00 00 1C 00 00-00 31 00 00 00 00 00 001.....	
0f0	00 3E 00 00 00 15 00 00-00 03 00 00 00 94 2C F4	>.....,ð	
100	50 10 00 00 00 44 41 54-41 00 46 3A 5C 4F 62 6A	P...DATA-F:\Obj	
110	49 44 2E 74 78 74 00 00-03 00 46 00 3A 00 5C 00	ID.txt...F:\..	
120	60 00 00 00 03 00 00 00 A0-58 00 00 00 00 00 00 00X.....	
130	64 65 73 6B 74 6F 70 2D-74 68 76 35 66 38 39 00	..\..\..\desktop-thv5f89-	
140	0E 05 1C BB 81 91 61 4A-B8 11 36 E0 5E 39 08 16	..»..aJ, 6âº..	
150	5C D2 2D 31 A8 9A E5 11-9B FA A4 BA DB BA 22 0F	\0-1"åúºÛº"	
160	0A 87 4A ED E0 AE 61 4E-93 63 11 90 FD 99 C7 E5	..JiàoaN.c..ÿ Çà	
170	5C D2 2D 31 A8 9A E5 11-9B FA A4 BA DB BA 22 0F	\0-1"åúºÛº"	
180	45 00 00 09 00 00 A0-39 00 00 00 31 53 50 53	E.....9..1SPS	
190	B1 16 6D 44 AD 8D 70 48-A7 48 40 2E A4 3D 78 8C	±..mD-pHSnE..H..	
1a0	1D 00 00 00 68 00 00 00-00 48 00 00 00 22 EF E2	..h..H..iâ	
1b0	3E 00 00 00 00 00 B0-DF 3B 00 00 00 00 00 00 00	>.....B;.....	
1c0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	

- 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



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 64 65 73-6B 74 6F 70 2D 74 76deskto-p-thv	
200 35 66 38 39 00 0A 87 4A-ED E0 AE 61 4E 93 63 11	5f89- JiāmāN-c	
210 90 FD 99 C7 E5 5C D2 2D-31 A8 9A E5 11 9B FA A4	ÿ Çåò-1- å-ùñ	
220 BA DB AA 22 OF 0A 87 4A-ED E0 AE 61 4E 93 63 11	Ü-.. JiāmāN-c	
230 90 FD 99 C7 E5 5C D2 2D-31 A8 9A E5 11 9B FA A4	ÿ Çåò-1- å-ùñ	
240 BA DB AA 22 OF 45 00 00-00 09 00 A0 39 00 00	Ü-.. E.... 9..	
150 00 5C 00 2E 00 2E 00 5C-00 44 00 65 00 73 00 6B	\...\.\-D-e-s-k	
160 00 74 00 6F 00 70 00 5C-00 4F 00 62 00 6A 00 49	t-o-p\.\-O-b-j-I	
170 00 44 00 2E 00 74 00 78-00 74 00 1F 00 43 00 3A	D-.t-x-t-..C:	
180 00 5C 00 55 00 73 00 65-00 72 00 73 00 5C 00 43	\-U-s-e-r-s\.\-D	
190 00 75 00 73 00 74 00 69-00 6F 00 20 00 48 00 75	u-s-t-i-n\.-H-u	
1a0 00 72 00 6C 00 62 00 75-00 74 00 5C 00 44 00 65	r-l-b-u-t\.\-D-e	
1b0 00 73 00 6B 00 74 00 6F-00 70 00 60 00 00 00 03	s-k-t-o-p\.\-....	
1c0 00 A0 58 00 00 00 00-00 00 64 65 73 6B 74	X....-deskt	
1d0 6F 70 2D 74 68 76 35 66-38 39 00 0A 87 4A ED E0	op-thv5f89- Jiā	
1e0 AE 61 4E 93 63 11 90 FD-99 C7 E5 91 DB 2D 31 A8	an-c\.\-çå-ö-1-	
1f0 9A E5 11 9B FA A4 BA DB-Ba 22 OF 0A 87 4A ED E0	å-..-ñ-ø-..-Jiā	
200 AE 61 4E 93 63 11 90 FD-99 C7 E5 91 DB 2D 31 A8	an-c\.\-çå-ö-1-	
210 9A E5 11 9B FA A4 BA DB-Ba 22 OF 45 00 00 00 09	å-..-ñ-ø-..-E....	

- 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



Original document	Renamed in same folder	New Object ID value
<p>Same Volume ID and Object ID values</p>	<p>Renamed in same folder</p> <p>Copy and Paste to a new folder</p>	<p>New Object ID value</p>

USB Storage Devices



```

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 64 65 73 6B 74 6F | X-----deskto
140| 70 2D 74 68 76 35 66 38-39 00 A2 E8 9F 4B A6 73 | p-thv5f89\é\Kiq
150| BE 44 A4 33 20 CE DA F0-1D A4 D0 D7 2D 31 A8 9A | Dm3 f04-8b*x-1\.
160| F5 11 9B FA A4 BA DB BA-22 0F A2 E8 9F 4B A6 73 | A-----*é\é\Kiq
170| BE 44 A4 33 20 CE DA F0-1D A4 D0 D7 2D 31 A8 9A | Dm3 f04-8b*x-1\.
180| E5 11 9B FA A4 BA DB BA-22 0F 45 00 00 00 09 00 | A-----*E\...
190| 00 A0 39 00 00 00 31 53-50 53 B1 16 6D 44 AD 8D | 9---1SPSx-mD-
1a0| 70 48 A7 48 40 2E A4 3D-78 8C 1D 00 00 00 68 00 | pHSH@.H=x-\h-
1b0| 00 00 00 48 00 00 00 7F-28 A4 1A 00 00 00 00 00 00 | ...-H-\(M\...
1c0| 00 10 00 00 00 00 00-00 00 00 00 00 00 00 00 00 | ...
1d0| 00 00 00 00 00 00 00 00 00 00 00 00 00 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 04 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 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 05 D8 2D 31 A8 9A | 0-1\.
180| E5 11 9B FA A4 BA DB BA-22 0F 45 00 00 00 09 00 | A-----*0-1\.
1a0| E5 11 9B FA A4 BA DB BA-22 0F 45 00 00 00 09 00 | A-----*0-1\.
1b0| 00 A0 39 00 00 00 31 53-50 53 B1 16 6D 44 AD 8D | 9---1SPSx-mD-
1c0| 70 48 A7 48 40 2E A4 3D-78 8C 1D 00 00 00 68 00 | pHSH@.H=x-\h-
1d0| 00 00 00 48 00 00 00 B0-C7 2D 31 A8 9A E5 11 9B | ...-H-\(C-1\...
1e0| FA A4 BA DB BA 22 0F 00-00 00 00 00 00 00 00 00 | ú\xÜ\...
1f0| 00 00 00 00 00 00 00 00 00 00 00 00 00 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



- 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\100EO35DV\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

The screenshot shows a Windows taskbar with several pinned icons. A context menu is open over one of the pinned items, showing a list of recently used documents. One document, "SaveAsTestDTtoOD.docx", is highlighted. A red dashed arrow points from the text "Right clicking will show a list of most recently used documents" to this menu item. Another red dashed arrow points from the text "Individual documents can also be pinned and will appear at the top of the menu" to the pinned icon on the taskbar.

- 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

The screenshot displays a forensic analysis interface. On the left, a file tree view shows a folder named "Evidence" containing "Files-FolderWebCacheTest.ad1". Inside this folder, there are various sub-directories and files, including "root", "Users", "Windows", and "CustomDestinations". Several files under "Windows\Recent\AutomaticDestinations" have their paths highlighted with red boxes. On the right, a detailed view of a "Shortcut File" is shown in a hex editor. The "Link target information" pane shows the local path as "C:\Users\Dustin Hurlbut\Documents\Uploads\WinkyAndBlinky.jpg". The "File attributes" pane indicates the file is an "Archive". Below these panes, a "File List" table is displayed, showing a list of files with columns for Name, Label, Item #, Ext, Path, Category, P-Size, MD5, SHA1, SHA256, Created, Accessed, and Modified. One row in the table is highlighted with a red box, corresponding to the file listed in the "Link target information" pane.

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

Jump List App IDs



- 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
9b9cc69c1c24e2b	Notepad
9d1f905ce5044aee	Edge Brower
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



File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256
f		872	Files-FolderWebCacheT...	Windows Shortcut	n/a	920 B	ca7e26...	5426d5...	d8996e...	
e		870	Files-FolderWebCacheT...	Windows Shortcut	n/a	977 B	05f37...	def744...	557866...	
DestList		7696	Files-FolderWebCacheT...	OLE Stream	n/a	49.32 KB	500cc...	f79de7...	4b1b57...	
d		871	Files-FolderWebCacheT...	Windows Shortcut	n/a	977 B	ae028...	e7dd00...	e09d02...	

File Content

```
JaNCoA"desktop-thv5f89?q\5C:\Users\{Dustin Hurlbut\Documents\Uploads\BAZINGA.txt)
JaNcDA"
JaNcDA"desktop-thv5f89o?@=9C:\Users\{Dustin Hurlbut\Desktop\Captures\Edge\UL02bDT.jpg}N0FKT
JaNcKA"desktop-thv5f89TA!,<C:\Users\{Dustin Hurlbut\Documents\Uploads\WinkyAndBlinky.jpg}Q&
JaNc A"
JaNc A"desktop-thv5f89?j9C:\Users\{Dustin Hurlbut\Desktop\Captures\Edge\DL04bWC.jpg:D
JaNcSA"
JaNcSA"desktop-thv5f89?09C:\Users\{Dustin Hurlbut\Desktop\Captures\Edge\DL04aWC.jpgM
```

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256
f		822	Files-FolderWebCacheT...	Windows Shortcut	n/a	1065 B	321277...	13F336...	4948c...	n/a
e		820	Files-FolderWebCacheT...	Windows Shortcut	n/a	1085 B	45249b...	570e2...	b07ad...	n/a
DestList		8351	Files-FolderWebCacheT...	OLE Stream	n/a	11.31 KB	d0393...	a5e36...	265b5d...	n/a
d		821	Files-FolderWebCacheT...	Windows Shortcut	n/a	1094 B	ea68a5...	bf7a5e...	88c7b5...	n/a

File Content

```
JaNCoA"desktop-thv5f89?q\5C:\Users\{Dustin Hurlbut\Documents\Uploads\BAZINGA.txt)
JaNcDA"
JaNcDA"desktop-thv5f89o?@=9C:\Users\{Dustin Hurlbut\Desktop\Captures\Edge\UL02bDT.jpg}N0FKT
JaNcKA"desktop-thv5f89TA!,<C:\Users\{Dustin Hurlbut\Documents\Uploads\WinkyAndBlinky.jpg}Q&
JaNc A"
JaNc A"desktop-thv5f89?j9C:\Users\{Dustin Hurlbut\Desktop\Captures\Edge\DL04bWC.jpg:D
JaNcSA"
JaNcSA"desktop-thv5f89?09C:\Users\{Dustin Hurlbut\Desktop\Captures\Edge\DL04aWC.jpgM
```

DestList

The screenshot shows the DestList file in a hex editor. The left pane displays a tree view of the file's contents, including various destination entries. A red box highlights the '32 byte Header' at the top of the list, and another red box highlights the 'Entries'. The right pane shows the hex dump of the file. A red box highlights a specific entry in the hex dump, which corresponds to the highlighted entry in the tree view. The entry contains a path string: 'J:\Windows\Recent\Jump List Test 04.ad1\...\PHYSICALDRIVE0\Partition 1 [245241MB]:System [NTFS]\[root]\Users\...\AppData\Roaming\Microsoft\Windows\Recent\DestList'. The bottom pane shows the file content, properties, and hex interpreter tabs.

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

DestList Win7-8 vs. Win10

The screenshot compares DestList files from Windows 8 and Windows 10. The left pane shows the Windows 8 DestList file, which has a header size of 114 bytes from the start of the record to the path string. The right pane shows the Windows 10 DestList file, which has a header size of 130 bytes. Both panes show the hex dump of the files, with a red box highlighting the path string 'Windows 10' in the Windows 10 file. The bottom pane shows the file content, properties, and hex interpreter tabs.

- 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

DestList – Header Entries

The diagram illustrates the structure of a DestList header. It shows two boxes at the top: 'Total Entries' (4-7) pointing to the first four bytes of a memory dump, and 'Pinned Entries' (8-11) pointing to the next four bytes. Below these, an arrow points from 'Last Issued Entry ID' (16-19) to the value '0010' in the dump, which corresponds to the fifth byte. The memory dump itself shows two rows of hex values: 0000 03 00 00 00 29 00 00 00 03 00 00 00 00 00 D8 42 and 0010 29 00 00 00 00 00 00 00-95 00 00 00 00 00 00 00. To the right, a screenshot of a pinned file list in Windows File Explorer is shown, listing four items: 'Pinned', 'UWPhotoDoc', 'JumpListTest 06.ad1/...', and 'JumpListTest 06.ad1/...'. Below the dump, a screenshot of a pinned OneDrive folder is shown, named 'PinnedOneDriveDoc.docx'.

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

Total Entries 4-7	Pinned Entries 8-11
-----------------------------	-------------------------------

0000 03 00 00 00 29 00 00 00 03 00 00 00 00 00 D8 42)0B
0010 29 00 00 00 00 00 00 00 00-95 00 00 00 00 00 00 00)

Last Issued Entry ID
16-19

Pinned

UWPhotoDoc

JumpListTest 06.ad1/...

JumpListTest 06.ad1/...

PinnedOneDriveDoc.docx

DestList Offsets Windows 10

SYNTRICATE

Beginning of Record (0)

NetBIOS Name (72-87)

Entry ID (88-95)

Last Access (100-107)

Pinned Status (108-111)

Path Size (128-129)

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.

0200	78 00 00 00 00 00	66 19-F1 11 13 99 A7 F9 0A 87	x.....f..ñ...\$ù...
0210	4A ED E0 AE 61 4E 93	63-11 90 FD 99 C7 E5 A3 E2	JiææaNc...y.çååä
0220	DC AD 0B 2D 4E 61 9B	CD-A4 BA DB BA 22 0F 0A 87	Ü...Jå...í...ø...e...
0230	4A ED E0 AE 61 4E 93	63-11 90 FD 99 C7 E5 A3 E2	JiææaNc...y.çååä
0240	DC AD 0B 2D 4A E5 11	9B CD-A4 BA DB BA 22 0F 0A 87	sktop-thvfs89...
0250	73 6B 74 6F 70 2D 74	68-76 35 66 38 39 00 10 87	...@PzEi
0260	00 00 00 00 00 00 00	00-0A 00 A0 50 TA C6 9E EC	b...VVV...
0270	D0 01 01 00 00 00 00	F4 FF FF FE 05 00 00 00 00 005-C:\.\U-
0280	00 00 00 00 00 00 00	35 00 43 00 3A 00 5C 00 55 00	s-e-r-s\Du-s...
0290	73 6B 65 00 72 00 73	00-5C 00 44 00 75 00 70 00 6C 00	t-i-n\H-u-r-l-
02A0	04 00 69 00 00 00 00	20 00-48 00 65 00 73 00 70 00	b-u-t\De-s-k-
02B0	62 00 70 00 00 00 00	74 00 5C 00-44 00 65 00 73 00 6B 00	t-o-p\S-t-e-
02C0	74 00 6F 00 70 00 5C 00	50 00-53 01 00 76 00 65 00	A-s-T-e-s-t-D-t-
02D0	00 00 73 00 54 00 65 00	00-73 00 74 00 44 00 54 00	t-o-O-D\d-o-c-
02E0	74 00 6F 00 4F 00 44 00	00-2E 00 64 00 6F 00 63 00	t-o-J-f-a-
02F0	78 00 00 00 00 00 06 14	AA 80 FB AF 3A 61 3A 0A 87	x.....ñ.ñ...

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 Content	Properties	Hex Interpreter

Display Time Zone: Eastern Daylight Time (From local machine)

SYNTRICATE

Jump List – Deleted Reference

The item you selected is unavailable. It might have been moved, renamed, or removed. Do you want to remove it from the list?

-
-

Name	Path
26	JumpListTest06.ad1\\.\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\root\Users\
27	JumpListTest_06.ad1\\.\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\root\Users\
28	JumpListTest_06.ad1\\.\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\root\Users\
29	JumpListTest_06.ad1\\.\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\root\Users\

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

Jump List – Deleted File

Recent

Name	Hex
22	105b0 00 2f 47 8f 00 2e 00 00-00 00 e4 c4 76 55 ff ..
23	105c0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 01 ..
24	105d0 59 2c 01 50 00 69 00 6e-00 65 00 64 00 47 ..
25	105e0 00 6e 00 54 00 61 00 73-00 65 00 62 00 61 00 ..
26	105f0 00 2e 00 64 00 6f 00 63-00 78 00 00 00 1c 00 ..
27	10600 00 00 00 1a 00 ef be 02-00 57 00 6f 00 72 00 ..
28	10610 00 2e 00 44 00 6f 00 63-00 75 00 6d 00 65 00 ..
29	10620 00 74 00 2e 00 31 00 32-00 00 00 1c 00 00 1c ..
	10630 00 7e 00 00 00 1c 00 00-00 01 00 1c 00 00 1c ..
	10640 00 33 00 00 00 00 00-00 7d 00 00 00 17 00 00 17 ..
	10650 00 03 00 00 9a 34 94-58 10 00 00 00 53 79 73 ..
	10660 74 65 6d 00 43 3a 5c 55-73 72 73 5c 44 75 ..
	10670 74 69 6e 20 48 75 72 6c-62 75 74 5c 44 65 73 ..
	10680 74 6f 70 5c 44 54 44 6f-63 73 5c 41 6e 6f 74 ..
	10690 65 72 46 62 6c 64 65 72-5c 59 69 62 65 64 ..
	106a0 5e 54 61 73 6b 62 61 72-2e 64 6f 63 78 00 00 ..
	106b0 00 00 00 03 00 00 00 00 00 00 00 00 00 00 64 ..
	106c0 65 73 6b 74 6f 70 2d 74-68 76 35 66 38 39 00 0a ..
	106d0 87 4a ed e0 ae 61 4e 93-63 11 90 fd 99 c7 e5 c3 ..
	106e0 cf df a4 e1 5a e5 11 9b-d5 a4 ba db ba 22 0f 0a ..

Search

Search Term: pinnedontaskbar

Warning

Not Found.

Find Next

Close

OK

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

User Pinned – File System

Link target information

Local Path	C:\Program Files\Microsoft Office 15\root\office15\POWERPNT.EXE
Volume Type	Fixed Disk
Volume Label	System
Volume Serial Number	5894-349A
File Size	1846960
Creation time	8/24/2015 9:46:55 PM +0000
Last write time	8/24/2015 9:48:42 PM +0000
Last access time	8/24/2015 9:48:41 PM +0000

File Explorer

Name	Created	Path
\$130	8/30 4:40:13 PM (2015-08-03 20:40:13 UTC)	JumplistTest05 Pinned and Count Test.ad1
AccessData FTK Imager.lnk	9/10/2015 10:13:36 PM (2015-09-10 17:01:36 UTC)	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
Command Prompt.lnk	9/10/2015 1:19:38 PM (2015-09-10 17:19:36 UTC)	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
Computer Management.lnk	9/10/2015 5:15:02 PM (2015-09-10 21:15:02 UTC)	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
Control Panel.lnk	8/4/2015 10:52:50 AM (2015-08-04 14:52:50 UTC)	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
desktop.ini	8/3/2015 4:40:13 PM (2015-08-03 20:40:13 UTC)	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
Event Viewer.lnk	8/4/2015 4:15:20 PM (2015-08-03 20:15:20 UTC)	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
File Explorer.lnk	8/3 20:40:13 UTC	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
Notepad.lnk	9/15 12:28:42 UTC	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
PowerPoint 2013.lnk	9-16 00:31:09 UTC	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
Registry Editor.lnk	8/4 12:38:44 UTC	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
Registry Viewer.lnk	8-27 00:28:15 UTC	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
Snipping Tool.lnk	8-04 20:54:56 UTC	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
TrueCrypt.lnk	9/12/2015 11:20:13 PM (2015-09-13 03:20:13 UTC)	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
Word 2013.lnk	8/26/2015 10:26:39 AM (2015-08-26 14:26:39 UTC)	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]
Wordpad.lnk	9/12/2015 8:18:12 PM (2015-09-13 00:18:12 UTC)	\V\PHYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]

- 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

Taskband

Name	Type	Data
FavoritesResolve	REG_BINARY	1A 06 00 00 4C 00 00 00 01 14 02 00 00
Favorites	REG_BINARY	00 C8 05 00 00 14 00 1F 80 9B D4 34 42 4
1190 00 00 00 5E 00 00 00 1D-00 EF BE 02 00 4D 00 69	-14...-M-
11A0 00 63 00 72 00 00 6F 00 73-00 6F 00 66 00 74 00 2E		c-r-o-s-o-f-t.-
11B0 00 57 00 69 00 6E 00 64-00 6F 00 77 00 73 00 53		W-i-n-d-o-w-s-
11C0 00 74 00 6F 00 72 00 65-00 5F 00 38 00 77 00 65 00 55		t-o-r-e-...-w-e-
11D0 00 6B 00 79 00 62 00 33-00 64 00 38 00 62 00 5F 00 55		...-h-3-d-a-
11E0 07 00 77 00 65 00 21 00 41-00 70 00 70 00 00 00 00 00		FD ..-w-e-...-A-p-p-
11F0 07 00 00 00 00 00 00 00 7A-03 00 00 4C 00 00 00 01	-z-L-....
1200 14 02 00 00 00 00 00 00 C0-00 00 00 00 00 00 46 83	-A-....-F-
1210 00 80 00 20 00 00 00 00 3A-3E 57 A2 E2 00 01 3A		...-..-?WS.ID-:
1220 3F 57 A7 2E CE 00 01 52-5C 78 A5 B5 BD 00 01 6E		?WS.ID-RxoxyD-n
1230 00 00 00 00 00 00 00 01-00 00 00 00 00 00 00 00 00	
1240 00 00 00 00 00 00 00 D8-01 3E 00 1F 80 C8 27 34	-Q-...-E'4
1250 1F 10 5C 10 42 AA 03 2E-E4 32 87 D6 68 26 00 01		..\B...-ar-Ohs-
1260 00 25 00 EE BE 12 00 00 00 CE 36 29 88 2C CE D0		-i-ik...-f6)-,iD
1270 01 32 99 1A 99 2C CE 00-01 32 99 1A 99 2C CE D0		-2...-iB-2...-,iB
1280 01 14 00 56 00 00 31 00 00-00 00 00 03 47 DD A6 11		..-V-1...-GY-.
1290 00 54 61 73 6B 00 61 72-00 40 00 00 00 04 EF		-Taskbar-8...-i
12A0 BE 03 47 07 A0 03 47 DD-A6 2E 00 00 00 CB EC 01		%-G-Y-GY-,...-E1-
12B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
12C0 00 00 00 00 00 8C DE 00 54-00 61 00 73 00 6B 00 42		...-P-T-a-s-k-B
12D0 00 61 00 72 00 00 16-00 46 01 32 00 6E 04 00 a-	-T-2...-.
12E0 00 5F 46 15 58 20 00 53-4E 49 50 49 7E 31 20		eF X-SNIPPI-
12F0 00 4E 4B 00 00 AE 00 09-00 04 00 EF BE 03 00		0 LNK-@...-14-G1-
1300 A0 03 47 DD A6 2E 00 00 00 E5 73 00 00 00 00 AE	-R-...-@
1320 CC 36 00 53 00 6E 00 00 00 00 00 00 00 00 6E 16 S-n-i-p-p-i-n		g- T-o-o-l-..-1
1330 00 67 00 20 00 00 00 00 00 00 00 00 00 00 6C		

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

CustomDestinations

Pointer to a search term
evidence, however it is possible
apps behavior with items it can
open and handle

Hex	Text	Filtered	Natural
15d0	61 80 00 00 00 00 68 00-74 00 74 00 70 00 3A 00		a.....h.t.t.p::
15e0	2F 00 2F 00 77 00 77 00-77 00 2E 00 6D 00 69 00		/ -www..mi
15f0	6B 00 65 00 62 00 61 00-66 00 6C 00 2E 00 63 00		k-e-b-a-l-l-c
1600	6F 00 6D 00 2F 00 65 00-78 00 70 00 65 00 64 00		o-m- <u>e-x-p-e-d</u> -
1610	69 00 74 00 69 00 6F 00-6E 00 73 00 2F 00 00 00		i-t-i-o-n-s/-
1620	00 00 1C 00 00 00 1A 00-EF BE 02 00 49 00 45 00	-t%_I-E-
1630	2E 00 48 00 54 00 54 00-50 00 00 00 00 00 00 00		.H-T-T-P-T...
1640	39 00 00 00 09 00 00 00-A0-2D 00 00 00 31 53 50 53		9.....-1SPS
1650	55 28 4C 9F 79 9F 39 4B-A8 07 E1 D4 3D E1 D5 F3		U(L-y-9K Đáô-đô
1660	11 00 00 00 07 00 00 00-00 00 00 00 00 00 FF FF 00	-vY
1670	00 00 00 00 00 00 00 00-00 00 00 00 00 01 14 02	
1680	00 00 00 00 00 00 C0 00-00 00 00 00 46 4C 00 00	A.....FL..
1690	00 01 14 02 00 00 00 00-C0 00 00 00 00 00 00 00	A.....
16a0	46 81 00 00 00 00 00 00-00 00 00 00 00 00 00 00		F.....
16b0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	
16c0	00 00 00 00 00 00 00 00-00 00 01 00 00 00 00 00	
16d0	00 00 00 00 00 00 00 00-FC 01 14 1F 00 80 00 00	ü.....
16e0	53 1C 87 A0 42 69 10 A2-EA 08 00 2B 30 30 9D E6		S.. Bi-eE-+00-e
16f0	01 61 80 00 00 00 66-00 74 00 74 00 70 00 3A 00		a.....h.t.t.p:
1700	00 0F 00 2F 00 77 00 77 00-77 00 2E 00 62 00 69		//www..bi
1710	66 00 67 00 67 00 63-00 6F 00 6D 00 2F 00 73 00		n-g..com/-s
1720	00 65 00 61 00 72 00 65-00 66 00 3F 00 71 00 3D		earch?n=
1730	00 6C 00 6F 00 72 00 65-00 74 00 61 00 35 00		l-or-e-to+m
1740	00 65 00 78 00 69 00 63-00 6F 00 2B 00 6C 00 00		e-x-i-c-o+-li
1750	76 00 65 00 61 00 62-00 6F 00 61 00 72 00 64		v-e-a-b-o-a-r-d
1760	00 2B 00 64 00 69 00 76-00 69 00 6E 00 67 00 26		+d-i-v-i-n-g-s

File List

Internet Explorer App ID

Cursor pos = 0

File Content | Properties | Hex Interpreter

File Explorer – Tracking

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...1SPS0...																
	<table border="1"> <thead> <tr> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr><td>Url</td><td>:2015081320150814: Dustin Hurlbut@file:///C:/Users/Dustin%20Hurlbut/Documents/Uploads/WinkyAndBlinky.jpg</td></tr> <tr><td>AccessedTime</td><td>8/13/2015 4:54:36 PM +0000</td></tr> <tr><td>ModifiedTime</td><td>8/13/2015 12:54:36 PM +0000</td></tr> <tr><td>ExpiryTime</td><td>9/8/2015 4:47:26 PM +0000</td></tr> <tr><td>SyncTime</td><td>8/13/2015 4:54:36 PM +0000</td></tr> <tr><td>AccessCount</td><td>1</td></tr> <tr><td>Directory</td><td>C:\Users\Dustin Hurlbut\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012015081320150814\</td></tr> </tbody> </table>	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\
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\																
Flags	0																
SyncCount	1																
Type	2097156																

SYNTRICATE

File Explorer – Tracking

Name	Type	Data
MRUListEx	REG_BINARY	06 00 00 00 07 00 00 0E 00 00 00 0C 00 00 00 0B 00
6	REG_BINARY	55 00 4C 00 30 00 32 00 64 00 44 00 54 00 2E 00 6A 00
7	REG_BINARY	55 00 4C 00 30 00 32 00 2E 00 6A 00 70 00 67 00 00 00
14	REG_BINARY	55 00 4C 00 30 00 32 00 61 00 2E 00 6A 00 70 00 67 00
12	REG_BINARY	55 00 4C 00 30 00 32 00 63 00 32 00 6E 00 64 00 20 00
11	REG_BINARY	55 00 4C 00 30 00 34 00 62 00 46 00 6F 00 6C 00 64 00
10	REG_BINARY	55 00 4C 00 30 00 34 00 61 00 46 00 6F 00 6C 00 64 00
5	REG_BINARY	55 00 4C 00 30 00 33 00 62 00 54 00 58 00 54 00 2E 00
16	REG_BINARY	55 00 4C 00 30 00 33 00 61 00 54 00 58 00 54 00 2E 00
9	REG_BINARY	55 00 4C 00 30 00 32 00 62 00 44 00 54 00 2E 00 6A 00
REG_BINARY	REG_BINARY	57 00 69 00 6E 00 6B 00 79 00 41 00 6E 00 64 00 42 00
8	REG_BINARY	44 00 4C 00 30 00 34 00 62 00 57 00 43 00 2E 00 6A 00
00 57 00 69 00 6E 00 6B 00-79 00 41 00 6E 00 64 00 W-i-n-k-y-A-n-d- 10 42 00 6C 00 69 00 6E 00-6B 00 79 00 2E 00 6A 00 B-l-i-n-k-y..j- 20 70 00 67 00 00 00 84 00-32 00 00 00 00 00 00 00 p-g-...-2-...- 30 00 00 00 00 57 69 6E 65-79 41 64 42 6C 69 6E ...WinkyAndBlin 40 6B 79 2E 6A 70 67 2E 6C-6E 6B 00 00 5E 00 09 00 ky.jpg.lnk-^...- 50 04 00 EF BE 00 00 00 00-00 00 00 00 2E 00 00 00 -i4-.....- 60 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00- 70 00 00 00 00 00 00 00 00-00 00 57 00 69 00 6E 00-Wini- 80 6B 00 79 00 41 00 6E 00-64 00 42 00 6C 00 69 00 k-y-A-n-d-B-l-i- 90 6E 00 6B 00 79 00 2E 00-6A 00 70 00 67 00 2E 00 n-k-y..j-p-g- a0 6C 00 6E 00 6B 00 00 00-26 00 00 00 l-n-k-4-...		

- 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



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.



Word Document

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

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)

Print Spool Files - .SHD Files



.SHD

- Account SID / RID
- Who Printed it
- Printer Used
- Doc Name

[HDRPrinter Serialization Format v.0 Spool File Interleaving Mode SPLFILE_COMMENT_INTERLEAVING_ON
Spool File Contents TYPE_XPS_MS_EPS011280395 (XP-520 Series) Letter (F0BEC2A1-F2E2-478D-97C9-17823E280395) InputBin FORMSOURCE RESDLU UnresDLL Orientation PORTRAIT Resolution Option360
PaperSize LETTER ColorMode Color24bpp Collated Color1 Color1 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]

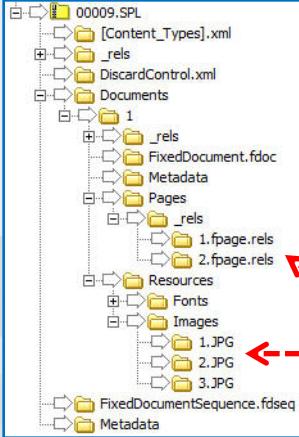
.SHD File Header

00	23	51	00	00	E0	00	00	00	00	28	00	09	00	00	00	#Q	â(
01	00	00	00	00	00	00	00	00	00	E0	07	00	00	00	00	00â
02	FE	07	00	00	00	00	00	00	00	1C	08	00	00	00	00	00p
03	00	00	00	00	00	00	00	00	00	6E	08	00	00	00	00	00n



Print Spool Files – Metadata

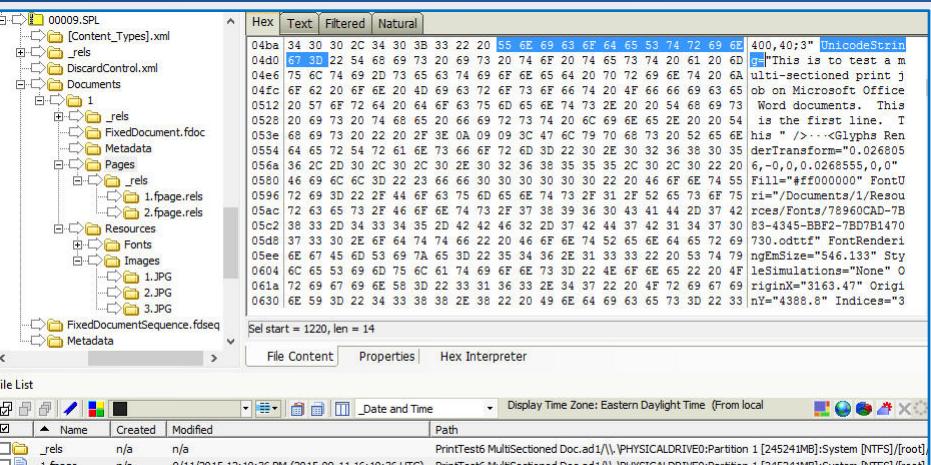
 SYNTRICATE



- 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

 SYNTRICATE



Name	Created	Modified	Path
_rels	n/a	n/a	PrintTest6 MultiSectioned Doc.ad1\ \PYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\[root]
1.page	9/11/2015 12:10:36 PM (2015-09-11 16:10:36 UTC)		PrintTest6 MultiSectioned Doc.ad1\ \PYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\[root]
2.page	n/a		PrintTest6 MultiSectioned Doc.ad1\ \PYSICALDRIVE0\Partition 1 [245241MB]\System [NTFS]\[root]

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

Print Spool Files – Resources

The screenshot shows the Print Spool Files - Resources interface. On the left, a file tree displays a folder structure under 'spool/PRINTERS'. A red circle highlights the 'Images' folder within the 'Resources' folder of a specific document's XML structure. To the right, a large image of a heron is shown. Below the tree, a 'File List' table shows two entries: '[0].piece' and '[1].last.piece'. A red arrow points from the circled 'Images' folder to the '[0].piece' entry in the file list, which includes the date and time information: '9/11/2015 12:10:36 PM (2015-09-11 16:10:36 UTC)'.

- 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

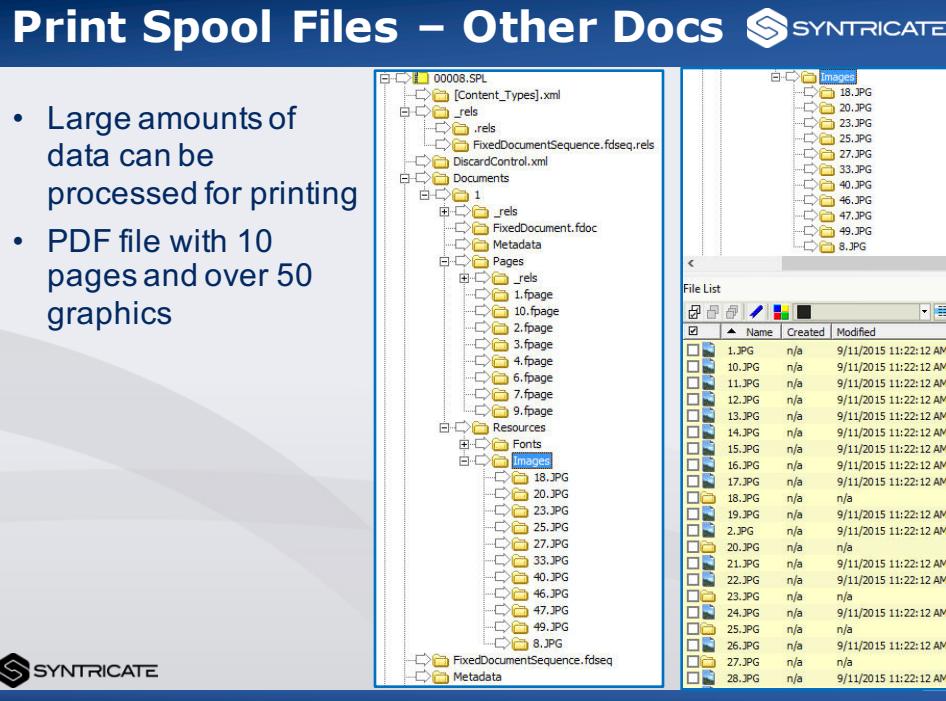
Print Spool Files – Resources

This screenshot is similar to the previous one but includes additional annotations. Red arrows point from the 'Images' folder in the file tree to the '[0].piece' entry in the file list and to the 'File Content' tab of the main window. The 'File Content' tab shows the XML structure of the document, with a red box highlighting the 'Images' section. Another red box highlights the 'File List' table, which now includes a third entry: '[1].last.piece'. The annotations explain that graphics pasted into the document are treated differently from ones added via the Insert > Picture menu.

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

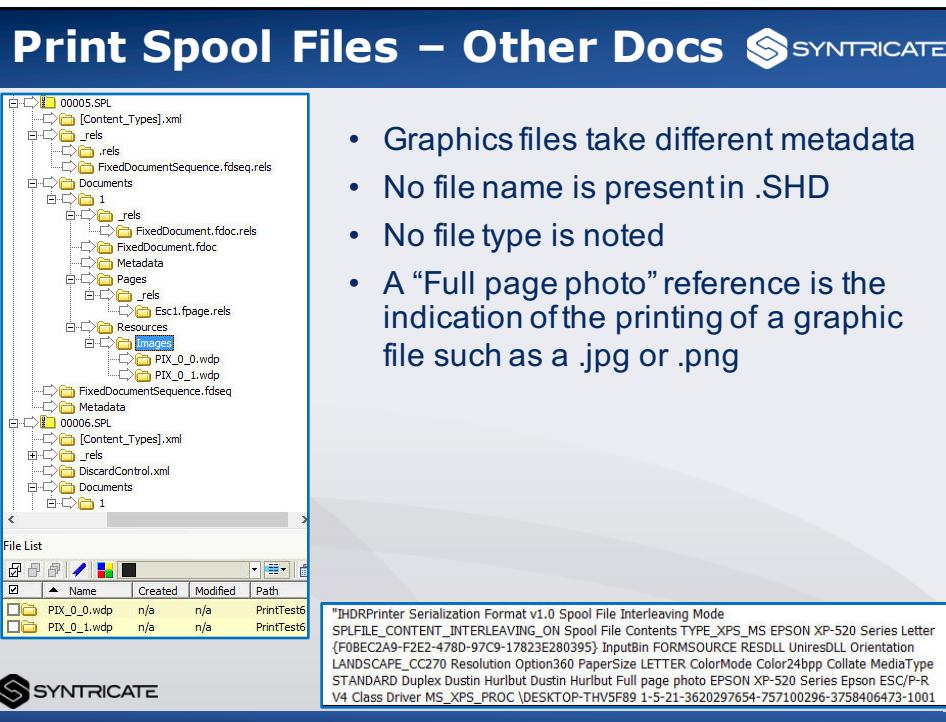
Print Spool Files – Other Docs

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



The screenshot shows a Print Spool File viewer interface. On the left, a tree view displays the structure of a print spool file, including subfolders like 00008.SPL, Content_Types.xml, .rels, FixedDocumentSequence.fdseq.rels, Documents, and a folder named '1'. Inside '1' are subfolders for .rels, FixedDocument.fdoc, Metadata, Pages (containing files 1.fpage through 9.fpage), Resources, and Images (containing files 18.JPG through 49.JPG). A separate 'Images' folder is also present. On the right, a 'File List' window shows a detailed list of files, primarily images, with columns for Name, Created, and Modified. The list includes files such as 1.JPG, 10.JPG, 11.JPG, 12.JPG, 13.JPG, 14.JPG, 15.JPG, 16.JPG, 17.JPG, 18.JPG, 19.JPG, 2.JPG, 20.JPG, 21.JPG, 22.JPG, 23.JPG, 24.JPG, 25.JPG, 26.JPG, 27.JPG, and 28.JPG, all created on 9/11/2015 at 11:22:12 AM.

Print Spool Files – Other Docs



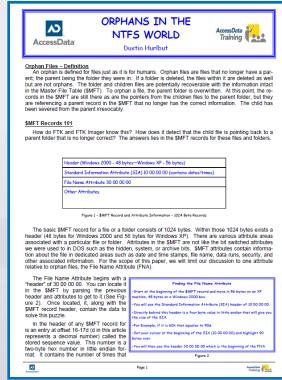
The screenshot shows a Print Spool File viewer interface similar to the previous one, but with a different file structure. It includes a tree view for 00005.SPL, 00006.SPL, and a folder named '1'. The '1' folder contains subfolders for .rels, FixedDocument.fdoc, Metadata, Pages, and Resources. Under Resources, there are two files: PIX_0_0.wdp and PIX_0_1.wdp. A 'File List' window shows two entries: PIX_0_0.wdp and PIX_0_1.wdp, both created on n/a by PrintTest6. At the bottom, a detailed footer message provides information about the IHDRPrinter Serialization Format v1.0, including the spool file interleaving mode, file contents, printer model (EPSON XP-520 Series Letter F08EC2A9-F2E2-478D-97C9-17823E280395), input bin (FORMSOURCE RESDLL UniresDLL), orientation (LANDSCAPE_CC270), resolution (Option360), paper size (LETTER), color mode (Color24bpp), collate (Collate), media type (STANDARD Duplex), driver (Dustin Hurlbut), and class driver (MS_XPS_PROC).

Print Spool Files – Post Print



Name	Date Modified	Size
00007.SPL		0
PP0d_mnt8m0jpwntuu_ixzy8ae.TMP	9/11/2015 2:52:57 PM	0
PP13l0npa0wlgwrf0oubg47ce.TMP	9/11/2015 2:53:21 PM	0
PP283xax4avvvl8bzv5tqybc.TMP	9/11/2015 2:53:21 PM	0
PP3pageo4op0e5fum9axhd63g.TMP	9/11/2015 2:53:21 PM	0
PP40jp1kuwh3rd5dy8jh70c.TMP	9/11/2015 2:53:21 PM	0
PP4ups_n07p0dkad740v6g9_.TMP	9/11/2015 2:53:21 PM	0
PP5j070b4ctq41smmsx8md.TMP	9/11/2015 2:53:21 PM	0
PP7cuysc7znfbowemcpu9bbmp5d.TMP	9/11/2015 2:53:21 PM	0
PP8vmjgfhfnwm942dc90628d.TMP	9/11/2015 2:53:21 PM	0
PPas2ph0ht9_n3q4z_5jxo4ivvc.TMP	9/11/2015 2:53:21 PM	0
Ppb9cxuwo4qvov0tux46tmgnpyb.TMP	9/11/2015 2:53:21 PM	0
PPba0eoku13mx2_0c3lkuac4lyb.TMP	9/11/2015 2:53:21 PM	0
PPctiqn03dikr1071bwvm3vdb.TMP	9/11/2015 2:53:21 PM	0
PPfm2z0l6cen9wotg0st_uuiwc.TMP	9/11/2015 2:53:21 PM	0
PPf_ezg1iwpb_g71pyu24vni.TMP	9/11/2015 2:53:21 PM	0
PPpt7d0tp5lgon82g9z2e74cy.TMP	9/11/2015 2:53:21 PM	0
PPkbv9ntrdrn92b_zj8h0_be.TMP	9/11/2015 2:53:21 PM	0
PPnmfvom8t0rnk1crq6x90ccr.TMP	9/11/2015 2:53:21 PM	0
PPokos245aw0ql10ghco03.pgc.TMP	9/11/2015 2:53:21 PM	0
PPoyqac3r55k21vokj4b8gfzq_b.TMP	9/11/2015 2:53:21 PM	0
PPp2lksgovv1fswubzc5h9bdmc.TMP	9/11/2015 2:53:21 PM	0
PPp3igspu0ycyzm0t5gy9enyj3c.TMP	9/11/2015 2:53:21 PM	0
PPp6m59ppimms9hie_ej9r3d9lc.TMP	9/11/2015 2:53:21 PM	0
PPq16ad12v74n5y5siz3e1b.TMP	9/11/2015 2:53:21 PM	0
PPrlv05qwklu_ga3y08uy837chc.TMP	9/11/2015 2:53:21 PM	0
PPrlv05qwklu_ga3y08uy837chc.TMP	9/11/2015 2:53:21 PM	0
PPRLV-1.TMP		0
PPscnewre78mih_851cg2av6pc.TMP	9/11/2015 2:53:21 PM	0
PPuda09guoylwudg2rhitzl.TMP	9/11/2015 2:53:21 PM	0
PPustmbflmb27f13jq71kqi_ljd.TMP	9/11/2015 2:53:21 PM	0
PPv_e6ze4z2rro0ppzyohe2kc.TMP	9/11/2015 2:53:21 PM	0
PPwa1543lzwfh6kymsmhe8ksc.TMP	9/11/2015 2:53:21 PM	0
PPx08etbkv0qijp9gpalml2v3b.TMP	9/11/2015 2:53:21 PM	0
PPxc9ec_ga8pfu_6niu4b1930.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



Disk 0	System (C) 239.49 GB NTFS Healthy (System, Boot, Page File, Active, Crash Dump, Primary P)
Disk 1	CODEMETER (E) 39 MB FAT32 Healthy (Active, Primary Partition)
Disk 2	WFR (G) 124 MB NTFS Healthy (Primary Partition)
Disk 3	FirstVHD (H) 7 MB NTFS Healthy (Primary Partition)



- 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



VHDs – Detection

Device Manager

SYSTEM Registry File

The screenshot shows the Windows Device Manager interface with the title "DESKTOP-THV5F89". Under the "Disk drives" section, two entries are visible: "Microsoft Virtual Disk" and "TOSHIBA MK325GDSY ATA Device". Below this, the "SYSTEM Registry File" is displayed in the Registry Editor. A specific key, "HKEY_LOCAL_MACHINE\DosDevices\H:", is selected, and its value data is shown as a binary sequence: 27 ad 74 9f 00 01 00 00 00 00. This value is highlighted with a red box.

VHDs – Detection

The screenshot shows the AccessData Forensic Toolkit interface. At the top, a hex dump of file data is displayed, showing binary values such as 000000, 33 C0 8E D0 BC 00 7C 8E, etc. Below this, the "Virtual HDD Identification" tool is open. It shows a "File List" containing two entries: "AnotherVHD.vhd" and "testing VHDs.vhd". A red dashed arrow points from the hex dump area towards this list. The "Virtual HDD Identification" tool also includes a sidebar with categories like OS/File System Files, Other Encryption Files, and User Types.

VHDs – Registry Artifacts

This screenshot shows a registry dump from a VHD. The main pane displays the registry keys under 'OpenSavePidlMRU' and 'vhd'. The 'vhd' key contains subkeys like '.wav', '.xls', '.xlsx', '.zip', 'Ribbon', 'RunMRU', 'Search', 'SearchPlatform', 'SharingMFU', and 'Shell Folders'. The 'Shell' key under 'vhd' has subkeys for 'Associations', 'BagMRU', 'Bags', and 'Desktop'. The 'Desktop' key contains items like '1', 'TabletPC', 'Windows Error Reporting', 'Windows Media', and 'Windows Media Foundation'. The bottom pane shows a detailed view of the 'Desktop' key, listing various registry entries with their names, types, and data. The data column includes binary hex values and ASCII representations of file paths and file names.

VHDs – Event Logs

This screenshot shows the Windows Event Log viewer. The left pane lists event sources: VerifyHardwareSecurity, VHDMP, Volume, VolumeSnapshot-Driver, Vpn Plugin Platform, VPN-Client, Wcmsvc, WebAuth, WeblO, WEPHOSTSVC, WFP, WiFiNetworkManager, Win32k, and Windows Defender. The right pane shows events for the 'VHDMP' source under the 'Operational' category. There are 16 events listed, all of type 'Information' with Event ID #1. The details pane shows a message: 'The VHD C:\Users\Dustin Hurlbut\Desktop\TestVHD.vhd has come online (surfaced) as disk number 3.' Below the event log is a bulleted list of facts about VHDs:

- 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



Hex Text Filtered Natural

Link target information

Local Path	E:\SOFTWARE\FTK_5.6.3_64_bit.iso
Volume Type	Fixed Disk
Volume Label	DustinBU010115
Volume Serial Number	5089-E771
File Size	2709323776
Creation time	6/15/2015 6:43:42 PM +0000
Last write time	6/15/2015 6:25:42 PM +0000

File Content Properties Hex Interpreter

Display Time Zone: Eastern Daylight Time (From local machine)

- 1 JumpListTest.06.ad1\\PhysicalDrive0:Partition 1 [245241MB]:System [NTFS] [root]\Users\Dustin Hurlbut\AppData\Roaming\Microsoft\Windows\JumpList\DestList
- 2 JumpListTest.06.ad1\\PhysicalDrive0:Partition 1 [245241MB]:System [NTFS] [root]\Users\Dustin Hurlbut\AppData\Roaming\Microsoft\Windows\JumpList\DestList
- 3 JumpListTest.06.ad1\\PhysicalDrive0:Partition 1 [245241MB]:System [NTFS] [root]\Users\Dustin Hurlbut\AppData\Roaming\Microsoft\Windows\JumpList\DestList
- 4 JumpListTest.06.ad1\\PhysicalDrive0:Partition 1 [245241MB]:System [NTFS] [root]\Users\Dustin Hurlbut\AppData\Roaming\Microsoft\Windows\JumpList\DestList

DestList

File Content (Hex View):

```

B4 A9 18 00 00 7E
CB 40 B0 6C 00 00
5C 00 3F 00 3F 00
0 1 \ 2 \ 3 \ . \ 5 \ C \ S \ I \
+ C \ d \ B \ 0 \ B \ 2 \ F \

```

- 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