

\$MFT Record:

```
■ Header
  - [0x1E43400] $MFT Record ID: 00AA00000000790D
  - [0x1E43400] Record Offset: 31732736
  - [0x00] Signature: FILE
  - [0x04] Offset to Update Sequence Array: 48
  - [0x06] Number of fix up byte pairs: 3
  - [0x08] $LogFile Sequence Number (LSN): 111841053577
  - [0x10] $MFT Record Sequence Nr: 170
  - [0x12] Hard Link Count: 1
  - [0x14] Offset to 1st Attribute: 56
  - [0x16] Allocation Status: 0x0001
    - Flag bit [14]: File,
    - Flag bit [15]: In Use
  - [0x18] Logical Size of MFT record: 416
  - [0x1C] Physical Size of MFT record: 1024
  - [0x20] Base Record: 0
  - [0x26] Base Record SeqNr: 0
  - [0x28] Next Available Attribute ID: 6
  - [0x2A] $MFT Record Nr: 30989
  - [0x30] Update sequence Number: 19475
  - [0x30] Update sequence/FixUp Value: 0x134C
  - [0x32] FixUp #1: 0x0000
  - [0x34] FixUp #2: 0x0000
  - [0x1FE] Check Value #1: 0x134C
  - [0x3FE] Check Value #2: 0x134C

■ Attributes
  - [0x038] ID: 0000, Type: (016) 10000000 - $Standard_Inf
  - [0x098] ID: 00005, Type: (048) 30000000 - $File_Name
  - [0x110] ID: 00004, Type: (064) 40000000 - $Object_ID
  - [0x138] ID: 00003, Type: (128) 80000000 - $Data
    - [0x13C] Attribute Length: 96
    - [0x140] Attribute Non-Resident Status: Non-Resident
    - [0x141] Length of Stream Name: 0
    - [0x142] Offset to Stream Name: 0
    - [0x144] Attribute Flags: 0x0000
    - [0x146] Attribute ID: 3
    - [0x148] Start VCN: 0
    - [0x150] End VCN: 8881151
    - [0x158] Datarun Offset: 64
    - [0x15A] Compression Unit Size: 0
    - [-----] Cluster Size: 4096
    - [0x160] Attribute Allocated Size: 36.377.198.592
    - [0x168] Attribute Actual Size: 36.377.198.592
    - [0x170] Attribute Initialized Size: 36.377.198.592
  - [0x178] DataRun: 4300847EC2B041094393EB00506E3504338
```

\$Data attribute's File Size:

```
[0x138] ID: 0003, Type: (128) 80000000 - $Data
  [0x13C] Attribute Length: 96
  [0x140] Attribute Non-Resident Status: Non-Resident
  [0x141] Length of Stream Name: 0
  [0x142] Offset to Stream Name: 0
  [0x144] Attribute Flags: 0x0000
  [0x146] Attribute ID: 3
  [0x148] Start VCN: 0
  [0x150] End VCN: 8881151
  [0x158] Datarun Offset: 64
  [0x15A] Compression Unit Size: 0
  [-----] Cluster Size: 4096
  [0x160] Attribute Allocated Size: 36.377.198.592
  [0x168] Attribute Actual Size: 36.377.198.592
  [0x170] Attribute Initialized Size: 36.377.198.592
```

	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00B	05	00	00	00	00	00	05	00	21	D7	C6	41	64	BB	D7	01	
00C	2F	BC	C4	C1	81	BB	D7	01	11	2D	61	C3	83	BB	D7	01	
00D	AE	9E	33	85	82	BB	D7	01	00	00	40	2C	03	00	00	00	
00E	00	00	40	2C	03	00	00	00	20	00	00	00	00	00	00	00	
00F	0D	00	57	00	69	00	6E	00	31	00	31	00	5F	00	34	00	
010	6B	00	2E	00	76	00	68	00	64	00	78	00	00	00	00	00	
011	40	00	00	00	28	00	00	00	00	00	00	00	00	00	04	00	
012	10	00	00	00	18	00	00	00	1D	2D	46	C2	5F	27	EC	11	
013	82	B6	A8	A1	59	56	C5	FC	80	00	00	00	60	00	00	00	
014	01	00	00	00	00	00	03	00	00	00	00	00	00	00	00	00	
015	FF	83	87	00	00	00	00	00	40	00	00	00	00	00	00	00	
016	00	00	40	78	08	00	00	00	00	00	40	78	08	00	00	00	

“0x 00 00 40 78 08 00 00 00”

Shell LNK pointing to the same file:

LECmd (*version 1.5.0.0*) reports wrong File Size:

```
[2023-12-21 16:54:50 INF] --- Header ---
[2023-12-21 16:54:50 INF]     Target created: 2021-10-07 10:15:30
[2023-12-21 16:54:50 INF]     Target modified: 2023-12-02 20:27:22
[2023-12-21 16:54:50 INF]     Target accessed: 2023-12-18 16:25:18

[2023-12-21 16:54:50 INF]     File size (bytes): 2.017.460.224
```

```
[2023-12-21 16:54:50 INF] -File ==> Win11_4k.vhdx
[2023-12-21 16:54:50 INF]     Short name: Win11_4k.vhdx
[2023-12-21 16:54:50 INF]     Modified: 2023-12-02 20:27:24
[2023-12-21 16:54:50 INF]     Extension block count: 1

[2023-12-21 16:54:50 INF] ----- Block 0 (BeEF0004) -----
[2023-12-21 16:54:50 INF] Long name: Win11_4k.vhdx
[2023-12-21 16:54:50 INF] Created: 2021-10-07 10:15:32
[2023-12-21 16:54:50 INF] Last access: 2023-12-18 15:37:02
[2023-12-21 16:54:50 INF] MFT entry/sequence #: 30989/170 (0x790D/0xAA)

[2023-12-21 16:54:50 INF] --- End Target ID information ---
```

So does Jumplist_Browser (up-to v.0.0.36.0):

```

[-] IDList Entry #002 [32]
  - ItemID Size: 102
  - ItemID Type: 32
  - File Size: 2017460224
  - Attributes: Archive (0x0020)
  - Ansi Name: Win11_4k.vhdx
  - Modified: 02-Dec-2023 20:27:24.00
  [-] Extension #0 Type: [BEEF0004]
    - Extension Size: 76
    - Extension Version: 9
    - Host OS: Windows 8.1/10/11
    - FS Hint: NTFS
    - Unicode Name: Win11_4k.vhdx
    - Created: 07-Oct-2021 10:15:32.00
    - Accessed: 18-Dec-2023 15:37:02.00
    - MFT Record Nr: 30989
    - MFT Record Sequence Nr: 170
    - Unknown value #1: 0x08000000
    - Unknown value #3: 0x9E8DB700
    - Extension Data
  - ItemID Data

```

Hex view of ItemID:

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	32	00	00	00	40	78	82	57	6C	A3	20	00	57	69	6E	31	2...@x,Wl£ .Win1
00000010	31	5F	34	6B	2E	76	68	64	78	00	4C	00	09	00	04	00	1_4k.vhdx.L....
00000020	EF	BE	47	53	F0	51	92	57	A1	7C	2E	00	00	00	0D	79	1%GSðQ'Wjy
00000030	00	00	00	00	AA	00	08	00	00	00	00	00	00	00	00	00a.....
00000040	00	00	00	00	9E	8D	B7	00	57	00	69	00	6E	00	31	00□..W.i.n.1.
00000050	31	00	5F	00	34	00	6B	00	2E	00	76	00	68	00	64	00	1._.4.k...v.h.d.
00000060	78	00	00	00	1C	00											x.....

Offsets 2 - 4 are the File size (32bit with max value: 4.294.967.295) – which in files with size within this limit works fine.

In this example it is: “0x 00 00 40 78” giving a File Size value of: 2.017.4460.224. But the real file size if greater than this value.

If we look at the ItemID’s Extension blocks (BE EF 00 xx) of the LNK, it has an Extension Type: [BEEF0004]:

LECmd:

```

----- Block 0 (BEEF0004) -----
Long name: Win11_4k.vhdx
Created: 2021-10-07 10:15:32
Last access: 2023-12-18 15:37:02
MFT entry/sequence #: 30989/170 (0x790D/0xAA)

```

Jumplist_Browser:

```

[+] Extension #0 Type: [BEEF0004]
  Extension Size: 76
  Extension Version: 9
  Host OS: Windows 8.1/10/11
  FS Hint: NTFS
  Unicode Name: Win11_4k.vhdx
  Created: 07-Oct-2021 10:15:32.00
  Accessed: 18-Dec-2023 15:37:02.00
  MFT Record Nr: 30989
  MFT Record Sequence Nr: 170
  Unknown value #1: 0x0800000000

```

Raw Hex:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	4C	00	09	00	04	00	EF	BE	47	53	F0	51	92	57	A1	7C
00000010	2E	00	00	00	0D	79	00	00	00	00	AA	00	08	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	9E	8D	B7	00	57	00
00000030	69	00	6E	00	31	00	31	00	5F	00	34	00	6B	00	2E	00
00000040	76	00	68	00	64	00	78	00	00	00	1C	00				

\$Reparse Point Tag: no tag

Extension Type: [BEEF0004]

\$MFT Record Nr: 30989

\$MFT Record Sequence Nr: 170

The 4 missing 65bit file size bytes

So, if we add the 4 bytes ("08 00 00 00") after the \$MFT information to the end of the 4 bytes in the ItemID above ("0x 00 00 40 78"), we get:

"0x 00 00 40 78" + "0x 08 00 00 00" => "0x 00 00 40 78 08 00 00 00" which in LE translates to

"0x 00 00 00 08 78 40 00 00" => 36.377.198.592:

HEX	8 7840 0000
DEC	36.377.198.592

The same example with PowerShell:

```

PS5.1 C:\>$a = Hex-toByteArray -Hex "00004078"
$b = Hex-toByteArray -Hex "08000000"
$c = $a + $b
[System.BitConverter]::ToInt64($c,0).ToString('N0')
36.377.198.592

```

```
■ IDList Entry #002 [32]
  ItemID Size: 102
  ItemID Type: 32
  File Size: 36.377.198.592
  Attributes: Archive (0x0020)
  Ansi Name: Win11_4k.vhdx
  Modified: 02-Dec-2023 20:27:24.00
  Extension #0 Type: [BEEF0004]
```

More examples:

Automatic Destinations stream:

Jumplist Explorer v.2.0.0.0 => wrong File Size:

General information		Target ID information		Extra blocks information	
Header					
Target created	2022-01-20 12:32:40		File size	2.760.257.515	
Target modified	2022-01-20 13:11:01		File attributes	FileAttributeArchive	
Target accessed	2022-01-20 18:22:48		Hot key		
Flags	HasTargetIdList, HasLinkInfo,IsUnicode, DisableKnownFolderTracking, AllowLinkToLink				
Show window	SwNormal		Icon index	0	
Link information					
Flags	VolumeIdAndLocalBasePath, CommonNetwo				
Volume information			Network share information		
Drive type	DriveFixed		Device name		
Serial number	6A9CCFC0		Share name		
Label	Data - Storage Pool		Provider type	WnnNetLanman	
Local path	F:\		Share flags	ValidNetType	
Common path	[REDACTED]\A QUIET PLACE PART II\A QUIET PLACE PART II.Title801.mp4				

Raw Hex of ItemID:

Actual 64bit File Size = 0xEB2F86A4 + 0x0A000000 => 45.709.930.475

```
[-] IDList Entry #006 [32]
  - ItemID Size: 192
  - ItemID Type: 32
  - File Size: 45.709.930.475
  - Attributes: Archive (0x0020)
  - Ansi Name: A QUIET~1.MP4
  - Modified: 20-Jan-2022 13:11:02.00
  [-] Extension #0 Type: [BEEF0004]
    - Extension Size: 118
    - Extension Version: 9
    - Host OS: Windows 8.1/10/11
    - FS Hint: NTFS
    - Unicode Name: A QUIET_PLACE_PART_II.Title801.mp4
    - Created: 20-Jan-2022 12:32:42.00
    - Accessed: 20-Jan-2022 18:22:36.00
    - MFT Record Nr: 1856576
    - MFT Record Sequence Nr: 5
    - Unknown value #3: 0x73471D00
    - Extension Data
  [+]- Extension #1 Type: [BEEF001A]
```

LNK Shortcut:

```
File size (bytes): 2.147.484.160
Flags: HasTargetIdList, HasLinkInfo, HasRelativePath

File attributes: FileAttributeArchive
Icon index: 0
Show window: SwNormal (Activates and displays the window when the window is minimized or maximized.)

Relative Path: ..\..\..\..\..\Desktop\SecretStuff.vhd

-File ==> SecretStuff.vhd
  Short name: SECRET~1.VHD
  Modified: 2019-03-13 02:07:06
  Extension block count: 1

  ----- Block 0 (Beef0004) -----
  Long name: SecretStuff.vhd
  Created: 2019-02-25 21:16:04
  Last access: 2019-03-13 18:13:56
  MFT entry/sequence #: 118829/6 (0x1D02D/0x6)
```

Actual File Size:

```
■ IDList Entry #002 [32]
├ ItemID Size: 106
├ ItemID Type: 32
└ File Size: 10.737.418.752
├ Attributes: Archive (0x0020)
└ Ansi Name: SECRET~1.VHD
└ Modified: 13-Mar-2019 02:07:06.00
■ Extension #0 Type: [BEEF0004]
├ Extension Size: 80
├ Extension Version: 9
└ Host OS: Windows 8.1/10/11
├ FS Hint: NTFS
└ Unicode Name: SecretStuff.vhd
└ Created: 25-Feb-2019 21:16:04.00
└ Accessed: 13-Mar-2019 18:13:56.00
└ MFT Record Nr: 118829
└ MFT Record Sequence Nr: 6
```