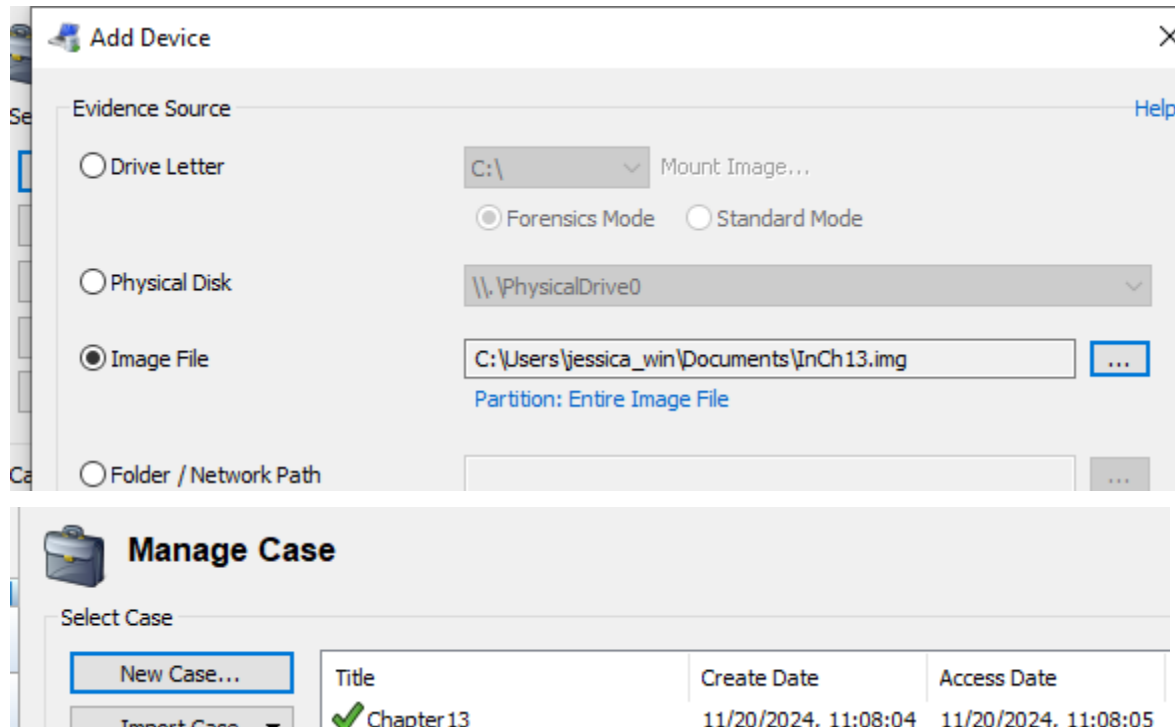


Task 1: Windows Prefetch Artifacts

Step 1: Setup Case



Successfully created new case with given image file.

Step 2: Identify Target Prefetch File

Icon	File Name	Type	Timestamp	Size
	DROPBOX 2.10.3.EXE-1BE8...	PF File	5/16/2020, 21:27:49.7892966	5/16/
	DROPBOX.EXE-587AFC15.pf	PF File	5/16/2020, 21:27:49.7922958	5/16/
	DROPBOX.EXE-AA3E8112.pf	PF File	5/16/2020, 21:27:49.7932968	5/16/
	DROPBOXDATA.EXE-D01D4...	PF File	5/16/2020, 21:27:49.7972966	5/16/

WinHex

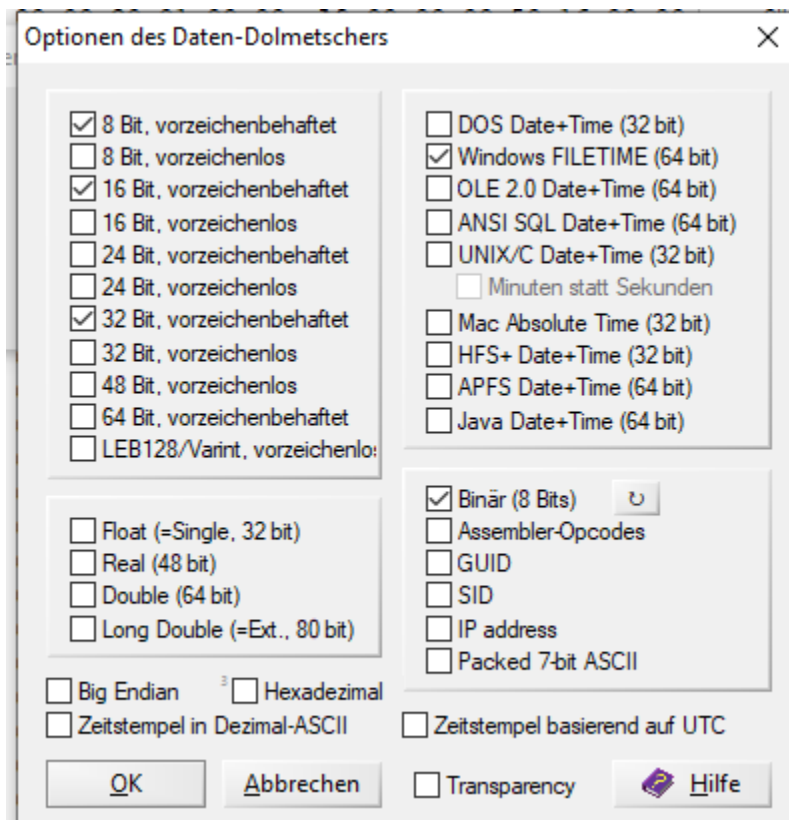
Datei Bearbeiten Suchen Navigation Ansicht Extras Specialist Optionen Fenster Hilfe 21.3

745B415EC366B474532473B989962B95.pf

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
0	1A	00	00	00	53	43	43	41	11	00	00	00	A4	A9	01	00		
16	44	00	52	00	4F	00	50	00	42	00	4F	00	58	00	2E	00	D	R
32	45	00	58	00	45	00	00	00	00	00	00	00	00	00	00	00	E	X
48	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
64	00	00	00	00	00	00	00	00	00	00	00	00	12	81	3E	AA		
80	00	00	00	00	30	01	00	00	A9	00	00	00	50	16	00	00		
96	6D	19	00	00	6C	47	01	00	4C	58	00	00	B8	9F	01	00		
112	01	00	00	00	EC	09	00	00	0F	00	00	00	01	00	00	00		
128	68	F5	48	2A	20	B1	CF	01	9D	61	FF	39	15	B1	CF	01		
144	CD	EA	83	3A	09	B1	CF	01	7F	48	9A	51	BA	AE	CF	01		
160	22	F7	C5	7A	B4	AE	CF	01	BC	66	05	75	AF	AE	CF	01		
176	7E	33	41	4F	AC	AE	CF	01	4F	BB	33	57	35	A8	CF	01		
192	00	8C	86	47	00	00	00	00	00	8C	86	47	00	00	00	00		
208	0B	00	00	00	05	00	00	00	03	00	00	00	00	00	00	00		
224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
304	00	00	00	00	A9	00	00	00	97	00	00	00	00	00	00	00		
320	32	00	00	00	00	02	00	00	E2	FD	01	00	00	00	01	00		

Successfully found target file and opened the .pf file in WinHex.

Step 3: Analyze Prefetch File



Not sure why my WinHex is in a different language, but I managed to follow the pictures and was able to apply the same settings.

745B415EC366B474532473B9...																
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	1A	00	00	00	53	43	43	41	11	00	00	00	A4	A9	01	00
00000010	44	00	52	00	4F	00	50	00	42	00	4F	00	58	00	2E	00
00000020	45	00	58	00	45	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	12	81	3E	AA
00000050	00	00	00	00	30	01	00	00	A9	00	00	00	50	16	00	00
00000060	6D	19	00	00	6C	47	01	00	4C	58	00	00	B8	9F	01	00
00000070	01	00	00	00	EC	09	00	00	0F	00	00	00	01	00	00	00
00000080	68	F5	48	2A	20	B1	CF	01	9D	61	FF	39	15	B1	CF	01
00000090	CD	EA	83	3A	09	B1	CF	01	7F	48	9A	51	BA	AE	CF	01
000000A0	22	F7	C5	7A	B4	AE	CF	01	BC	66	05	75	AF	AE	CF	01
000000B0	7E	33	41	4F	AC	AE	CF	01	4F	BB	33	57	35	A8	CF	01
000000C0	00	8C	86	47	00	0	Data Interpreter 8 Bit (±): 104 16 Bit (±): -2,712 32 Bit (±): 709,424,488 Binary: 01101000 FILETIME: 08/06/2014 02:43:12						47	00	00	00
000000D0	0B	00	00	00	05	0							00	00	00	00
000000E0	00	00	00	00	00	0							00	00	00	00
000000F0	00	00	00	00	00	0							00	00	00	00
00000100	00	00	00	00	00	0							00	00	00	00
00000110	00	00	00	00	00	0							00	00	00	00
00000120	00	00	00	00	00	0							00	00	00	00
00000130	00	00	00	00	A9	0							00	00	00	00

Documented the runtime at offset 0x80.

view tools specialist options window help

745B415EC366B474532473B9...

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	1A	00	00	00	53	43	43	41	11	00	00	00	A4	A9	01	01
00000010	44	00	52	00	4F	00	50	00	42	00	4F	00	58	00	2E	01
00000020	45	00	58	00	45	00	00	00	00	00	00	00	00	00	00	01
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01
00000040	00	00	00	00	00	00	00	00	00	00	00	00	12	81	3E	A1
00000050	00	00	00	00	30	01	00	00	A9	00	00	00	50	16	00	01
00000060	6D	19	00	00	6C	47	01	00	4C	58	00	00	B8	9F	01	01
00000070	01	00	00	00	EC	09	00	00	0F	00	00	00	01	00	00	01
00000080	68	F5	48	2A	20	B1	CF	01	8D	61	FF	39	15	B1	CF	01
00000090	CD	EA	83	3A	09	B1	CF	01	7F	48	9A	51	BA	AE	CF	01
000000A0	22	F7	C5	7A	B4	AE	CF	01	BC	66	05	75	AF	AE	CF	01
000000B0	7E	33	41	4F	AC	AE	CF	01	4F	BB	33	57	35	A8	CF	01
000000C0	00	8C	86	47	00	00	00	00	47	00	00	00	00	00	00	01
000000D0	0B	00	00	00	05	00	00	00	00	00	00	00	00	00	00	01
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01
00000130	00	00	00	00	A9	00	00	00	00	00	00	00	00	00	00	01
00000140	32	00	00	00	00	02	00	00	E2	FD	01	00	00	00	01	01
00000150	32	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01

Data Interpreter

8 Bit (±): -99
 16 Bit (±): 24,989
 32 Bit (±): 973,037,981
 Binary: 10011101
 FILETIME: 08/06/2014 01:24:54

Documented offset 0x88.

745B415EC366B474532473B9...																
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	1A	00	00	00	53	43	43	41	11	00	00	00	A4	A9	01	00
00000010	44	00	52	00	4F	00	50	00	42	00	4F	00	58	00	2E	00
00000020	45	00	58	00	45	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	12	81	3E	AA
00000050	00	00	00	00	30	01	00	00	A9	00	00	00	50	16	00	00
00000060	6D	19	00	00	6C	47	01	00	4C	58	00	00	B8	9F	01	00
00000070	01	00	00	00	EC	09	00	00	0F	00	00	00	01	00	00	00
00000080	68	F5	48	2A	20	B1	CF	01	9D	61	FF	39	15	B1	CF	01
00000090	CD	EA	83	3A	09	B1	CF	01	7F	48	9A	51	BA	AE	CF	01
000000A0	22	F7	C5	7A	B4	AE	CF	01	BC	66	05	75	AF	AE	CF	01
000000B0	7E	33	41	4F	AC	AE	CF	01	4F	BB	33	57	35	A8	CF	01
000000C0	00	8C	86	47	00	00	00	00	00	8C	86	47	00	00	00	00
000000D0	0B	00	00	00	05	00	00	00	03	00	00	00	00	00	00	00
000000E0	00	Data Interpreter						00	00	00	00	00	00	00	00	00
000000F0	00							00	00	00	00	00	00	00	00	00
00000100	00							00	00	00	00	00	00	00	00	00
00000110	00							00	00	00	00	00	00	00	00	00
00000120	00							00	00	00	00	00	00	00	00	00
00000130	00	Binary: 00001011						00	97	00	00	00	00	00	00	00
00000140	32	FILETIME: 01/01/1601						00	E2	FD	01	00	00	00	01	00
00000150	A9	00:35:47						00	2E	00	00	00	66	00	00	00
00000160	35	00	00	00	00	02	00	00	06	43	01	00	00	00	02	00
00000170	E7	00	00	00	59	00	00	00	45	00	00	00	D2	00	00	00

Documented offset at 0xD0 (208).