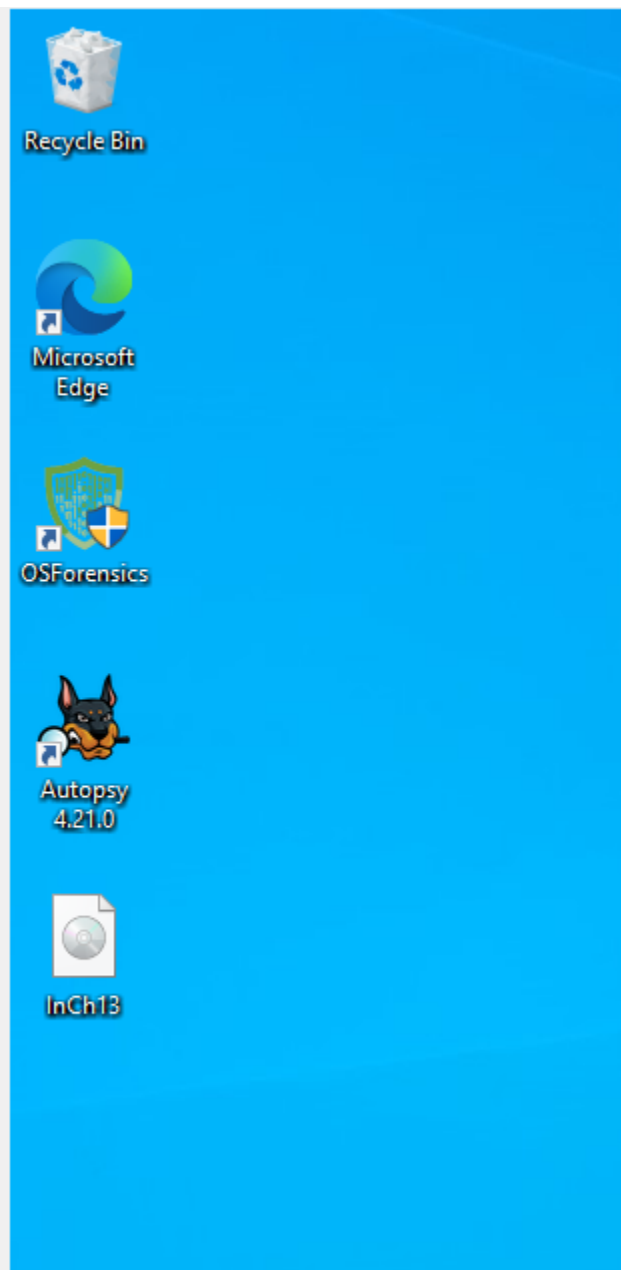
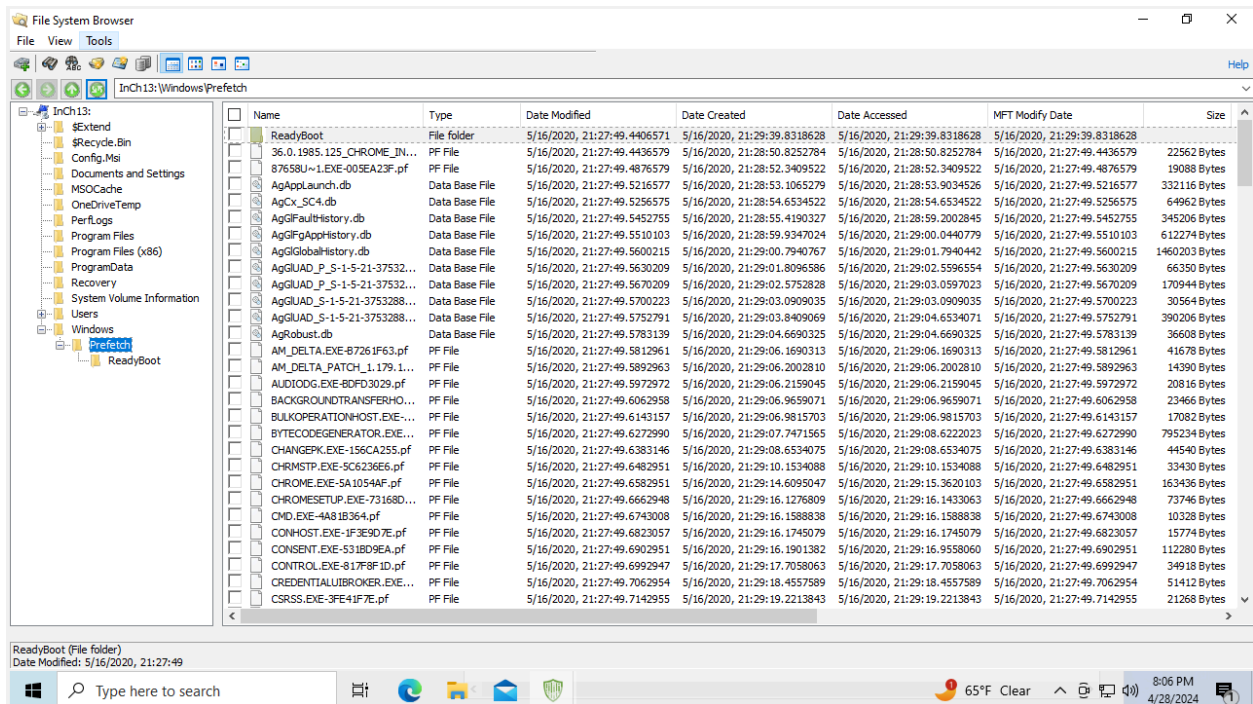


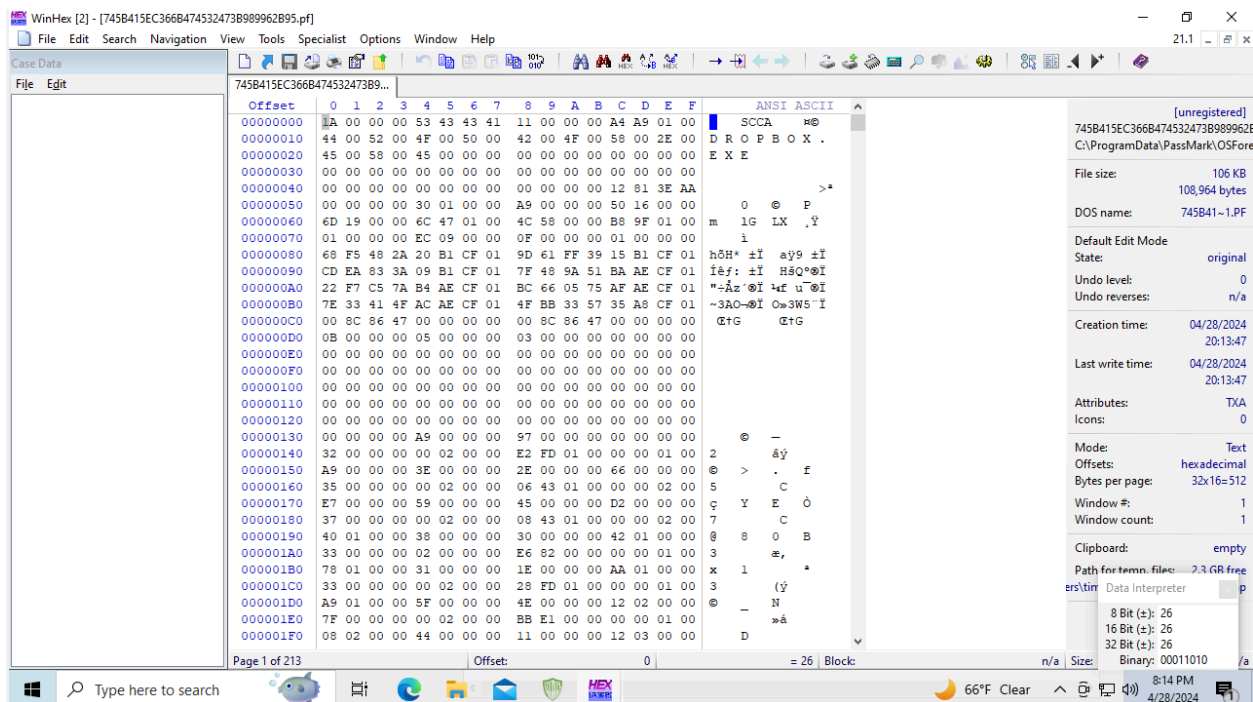
Task 1:



I have downloaded and extracted InCh13.

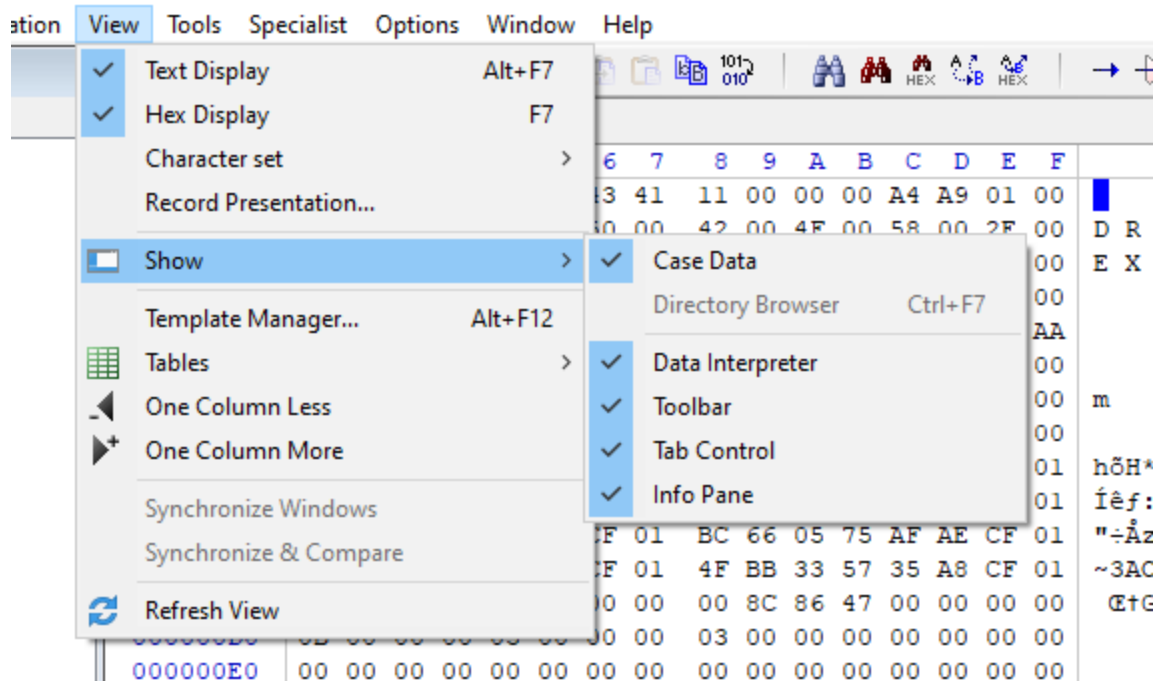


In this step, I have created a new case and added the InCh13 image to it. Here I am in the Windows/Prefetch folder.

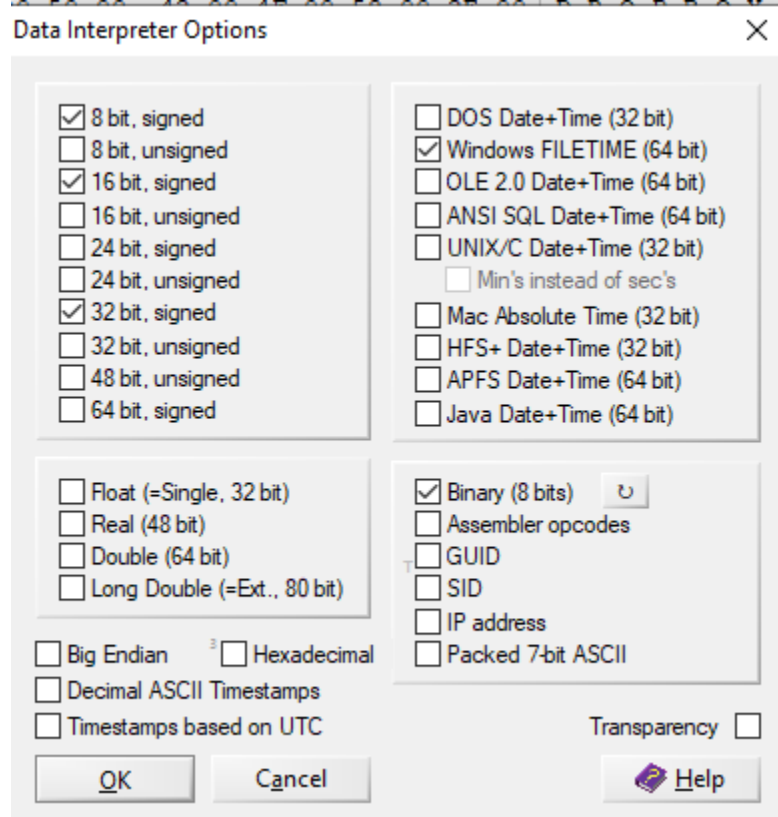


I have found “ROPBOX.EXE-AA3E8112.pf” and have opened it in WinHex.

474532473B989962B95.pf]



Here we can see that the data interpreter window is open.



Here, I am displaying the windows timestamp.

745B415EC366B474532473B9...																	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	1A	00	00	00	53	43	43	41	11	00	00	00	A4	A9	01	00	SCCA H@
00000016	44	00	52	00	4F	00	50	00	42	00	4F	00	58	00	2E	00	D R O P B O X .
00000032	45	00	58	00	45	00	00	00	00	00	00	00	00	00	00	00	E X E
00000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000064	00	00	00	00	00	00	00	00	00	00	00	12	81	3E	AA		>^
00000080	00	00	00	00	00	00	00	00	00	00	00	50	16	00	00	00	0 © P
00000096	6D	19	00	00	00	00	00	00	58	00	00	B8	9F	01	00	00	m 1G LX ,ÿ
00000112	01	00	00	00	00	00	00	00	00	00	00	01	00	00	00	00	i
00000128	68	F5	48	2A	00	00	00	00	61	FF	39	15	B1	CF	01	00	hõH* ±ÿ aÿ9 ±ÿ
00000144	CD	EA	83	3A	00	00	00	00	48	9A	51	BA	AE	CF	01	00	íêf: ±ÿ HšQ°@ÿ
00000160	22	F7	C5	7A	00	00	00	00	66	05	75	AF	AE	CF	01	00	"÷Äz'@ÿ ¼f u~@ÿ
00000176	7E	33	41	4F	AC	AE	CF	01	4F	BB	33	57	35	A8	CF	01	~3AO~@ÿ O»3W5"ÿ
00000192	00	8C	86	47	00	00	00	00	00	8C	86	47	00	00	00	00	Ë+G Ë+G
00000208	0B	00	00	00	05	00	00	00	03	00	00	00	00	00	00	00	
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000304	00	00	00	00	A9	00	00	00	97	00	00	00	00	00	00	00	© —
00000320	32	00	00	00	00	02	00	00	E2	FD	01	00	00	00	01	00	2 âÿ
00000336	A9	00	00	00	3E	00	00	00	2E	00	00	00	66	00	00	00	© > . f
00000352	35	00	00	00	00	02	00	00	06	43	01	00	00	00	02	00	5 C
00000368	E7	00	00	00	59	00	00	00	45	00	00	00	D2	00	00	00	ç Y E Ò
00000384	37	00	00	00	00	02	00	00	08	43	01	00	00	00	02	00	7 C
00000400	40	01	00	00	38	00	00	00	30	00	00	00	42	01	00	00	@ 8 0 B
00000416	33	00	00	00	02	00	00	00	E6	82	00	00	00	00	01	00	3 æ,
00000432	78	01	00	00	31	00	00	00	1E	00	00	00	AA	01	00	00	x 1 ^
00000448	33	00	00	00	00	02	00	00	28	FD	01	00	00	00	01	00	3 (ÿ
00000464	A9	01	00	00	5F	00	00	00	4E	00	00	00	12	02	00	00	© — N
00000480	7F	00	00	00	00	02	00	00	BB	E1	00	00	00	00	01	00	»á
00000496	08	02	00	00	44	00	00	00	11	00	00	00	12	03	00	00	D

Data Interpreter

8 Bit (±): 0

16 Bit (±): 0

32 Bit (±): 0

Binary: 00000000

FILETIME: 01/02/1601

12:16:07

Page 1 of 213

Offset: 80

= 0 Block

I am at offset 0x80 and can see the most recent runtime was 12:16:07.

745B415EC366B474532473B9...

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	1A	00	00	00	53	43	43	41	11	00	00	00	A4	A9	01	00	SCCA
00000016	44	00	52	00	4F	00	50	00	42	00	4F	00	58	00	2E	00	D R O P B O X .
00000032	45	00	58	00	45	00	00	00	00	00	00	00	00	00	00	00	E X E
00000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000064	00	00	00	00	00	00	00	00	00	00	00	12	81	3E	AA		>^
00000080	00	00	00	00	00	00	00	00	00	00	00	50	16	00	00		0 P
00000096	6D	19	00	00	16	Bit (±): 169			58	00	00	B8	9F	01	00		m 1G LX ,Y
00000112	01	00	00	00	32	Bit (±): 169			00	00	00	01	00	00	00		i
00000128	68	F5	48	2	Binary: 10101001				61	FF	39	15	B1	CF	01		hōH* ±I aŷ9 ±I
00000144	CD	EA	83	3	FILETIME: 01/29/1601				48	9A	51	BA	AE	CF	01		īēf: ±I HšQ°@I
00000160	22	F7	C5	7	09:28:05				66	05	75	AF	AE	CF	01		"-Åz'@I t4f u`@I
00000176	7E	33	41	4F	AC	AE	CF	01	4F	BB	33	57	35	A8	CF	01	~3AO~@I O»3W5" I
00000192	00	8C	86	47	00	00	00	00	00	8C	86	47	00	00	00	00	ÆtG
00000208	0B	00	00	00	05	00	00	00	03	00	00	00	00	00	00	00	
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000304	00	00	00	00	A9	00	00	00	97	00	00	00	00	00	00	00	© -
00000320	32	00	00	00	00	02	00	00	E2	FD	01	00	00	00	01	00	2 äŷ
00000336	A9	00	00	00	3E	00	00	00	2E	00	00	00	66	00	00	00	© > . f
00000352	35	00	00	00	00	02	00	00	06	43	01	00	00	00	02	00	5 C
00000368	E7	00	00	00	59	00	00	00	45	00	00	00	D2	00	00	00	ç Y E Ò
00000384	37	00	00	00	00	02	00	00	08	43	01	00	00	00	02	00	7 C
00000400	40	01	00	00	38	00	00	00	30	00	00	00	42	01	00	00	@ 8 0 B
00000416	33	00	00	00	02	00	00	00	E6	82	00	00	00	00	01	00	3 æ,
00000432	78	01	00	00	31	00	00	00	1E	00	00	00	AA	01	00	00	x 1 ^
00000448	33	00	00	00	00	02	00	00	28	FD	01	00	00	00	01	00	3 (ŷ
00000464	A9	01	00	00	5F	00	00	00	4E	00	00	00	12	02	00	00	@ - N
00000480	7F	00	00	00	00	02	00	00	BB	E1	00	00	00	00	01	00	»ä
00000496	08	02	00	00	44	00	00	00	11	00	00	00	12	03	00	00	D

Page 1 of 213 Offset: 88 = 169 Block: 80 - 95 Size: 16

[unregistered]
745B415EC366B474532473B989962E
C:\ProgramData\PassMark\OSFore

File size: 106 KB
108,964 bytes

DOS name: 745B41~1.PF

Default Edit Mode: original

State: original

Undo level: 0

Undo reverses: n/a

Creation time: 05/02/2024 22:41:44

Last write time: 05/02/2024 22:41:44

Attributes: TXA

Icons: 0

Mode: hexadecimal

Offsets: decimal

Bytes per page: 32x16=512

Window #: 1

Window count: 1

Clipboard: empty

Path for temp. files: 1.7 GB free
ers\timothyd\AppData\Local\Temp

I am now at offset 0x88 and the modification date was 5/02/2024.

0