

Maria Valencia

Csc 153

Lab 13

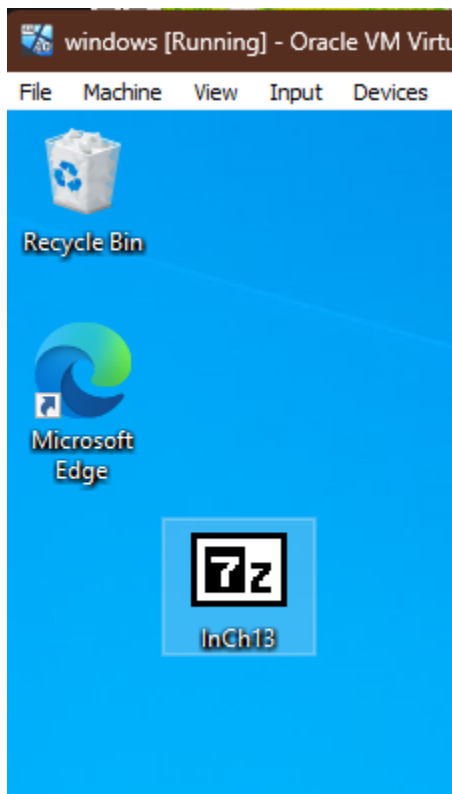
Cloud Forensics

Task 1 – Windows Prefetch Artifacts

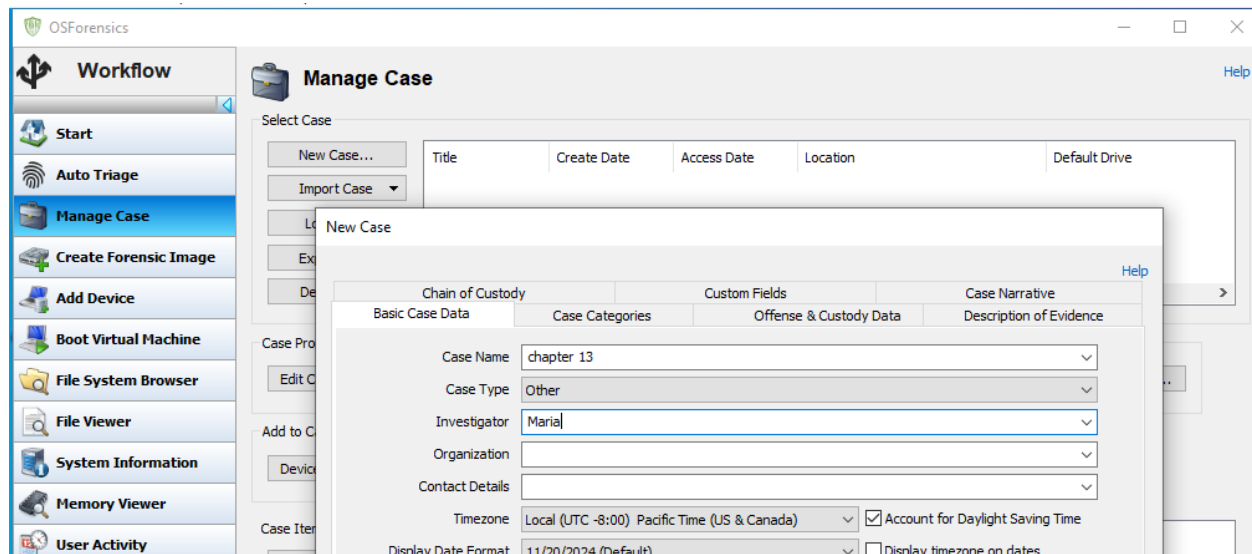
In this task you will find an application's MAC dates and counter using OSForensics and WinHex Data Interpreter in your Windows VM.

Step 1: Setup Case

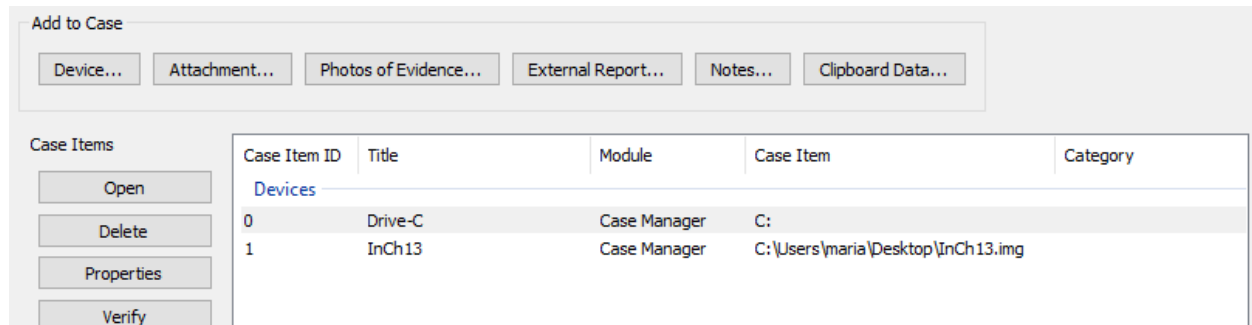
From your Windows VM, download the "InCh13.exe" to the machine. Run the EXE to extract the InCh13.img file.



Start OSForensics and create a new case named "chapter13" with your name as the investigator.

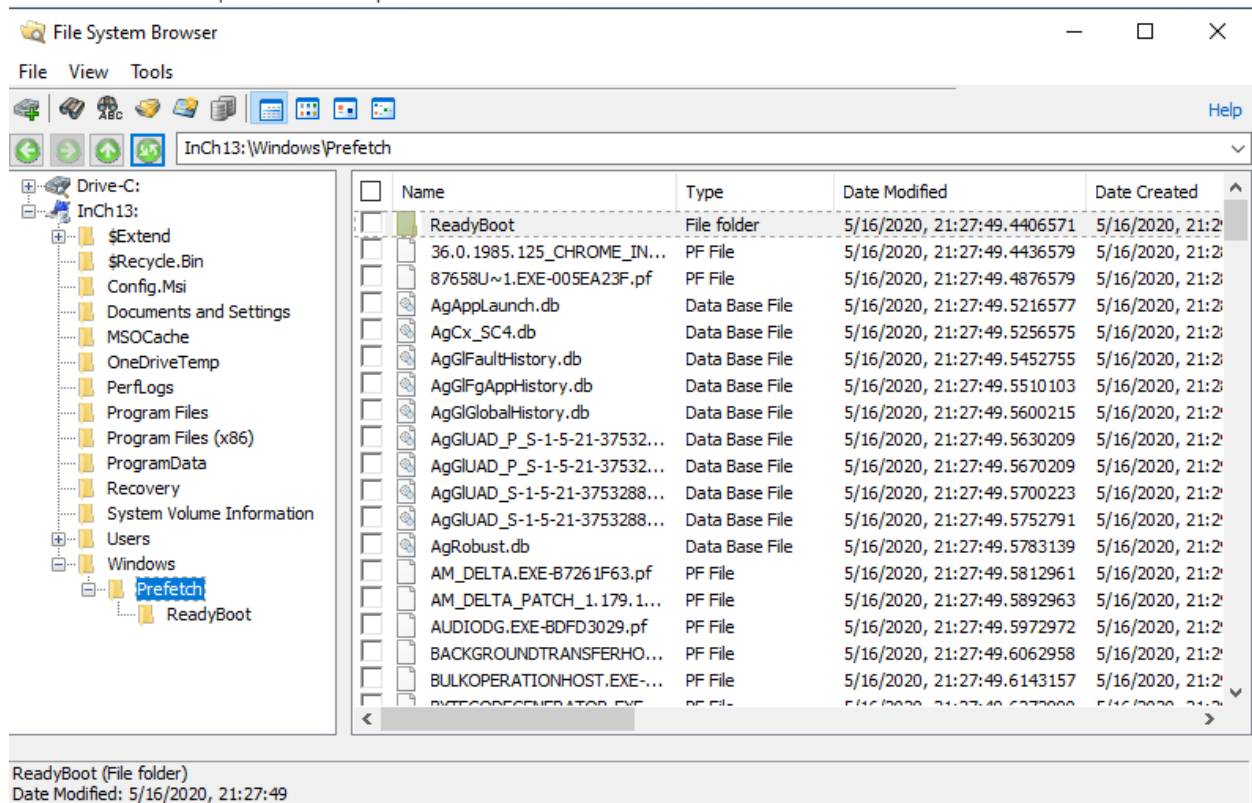


Add the "InCh13.img" as a device to the case using the "Device..." button. Select "Image File" and choose the path to your "InCh13.img" file.

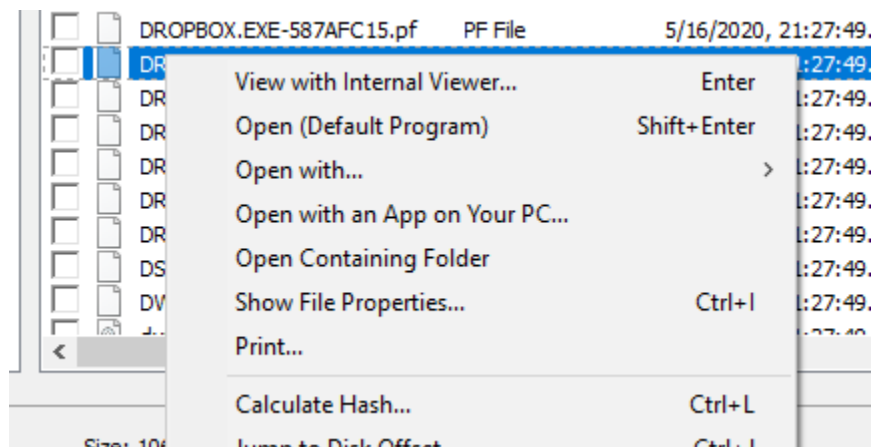


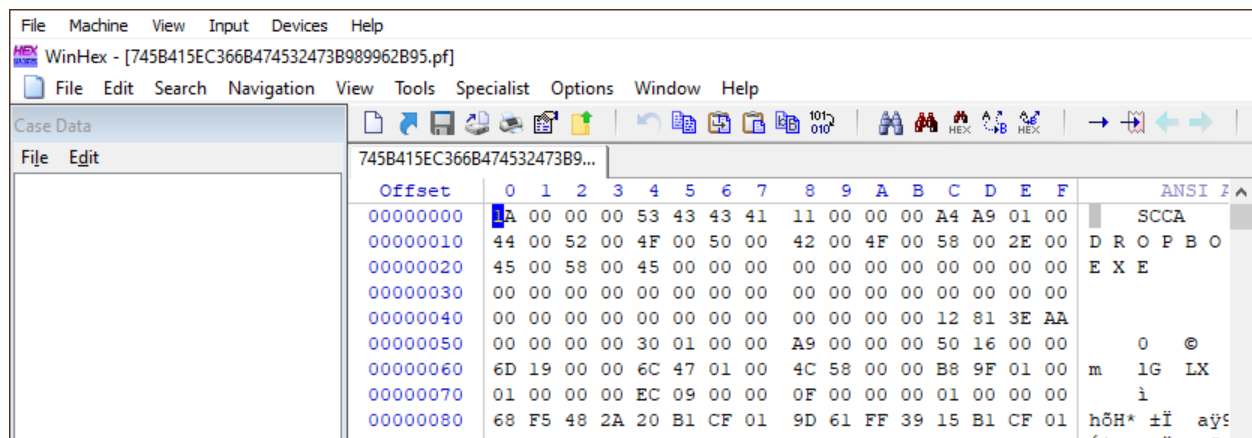
Step 2: Identify Target Prefetch File

With the image added to the case, select the "File System Browser" on the left navigation pane. Expand the navigation pane and select Windows/Prefetch folder.



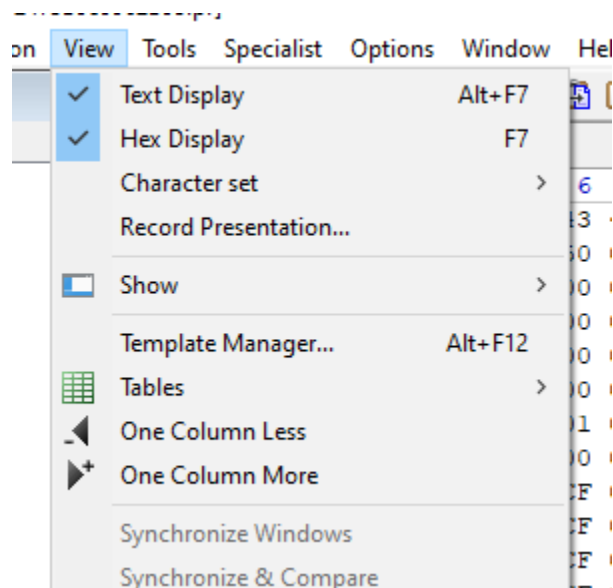
Scroll through the listings and find the "DROPBOX.EXE-AA3E8112.pf" file. Right click the file and choose "Open with..." and find the WinHex application (C:\Program Files\WinHex\winhex.exe").



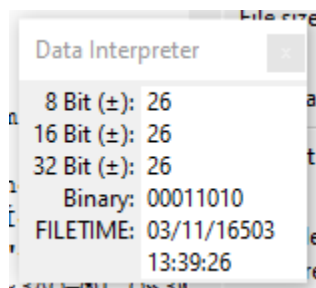
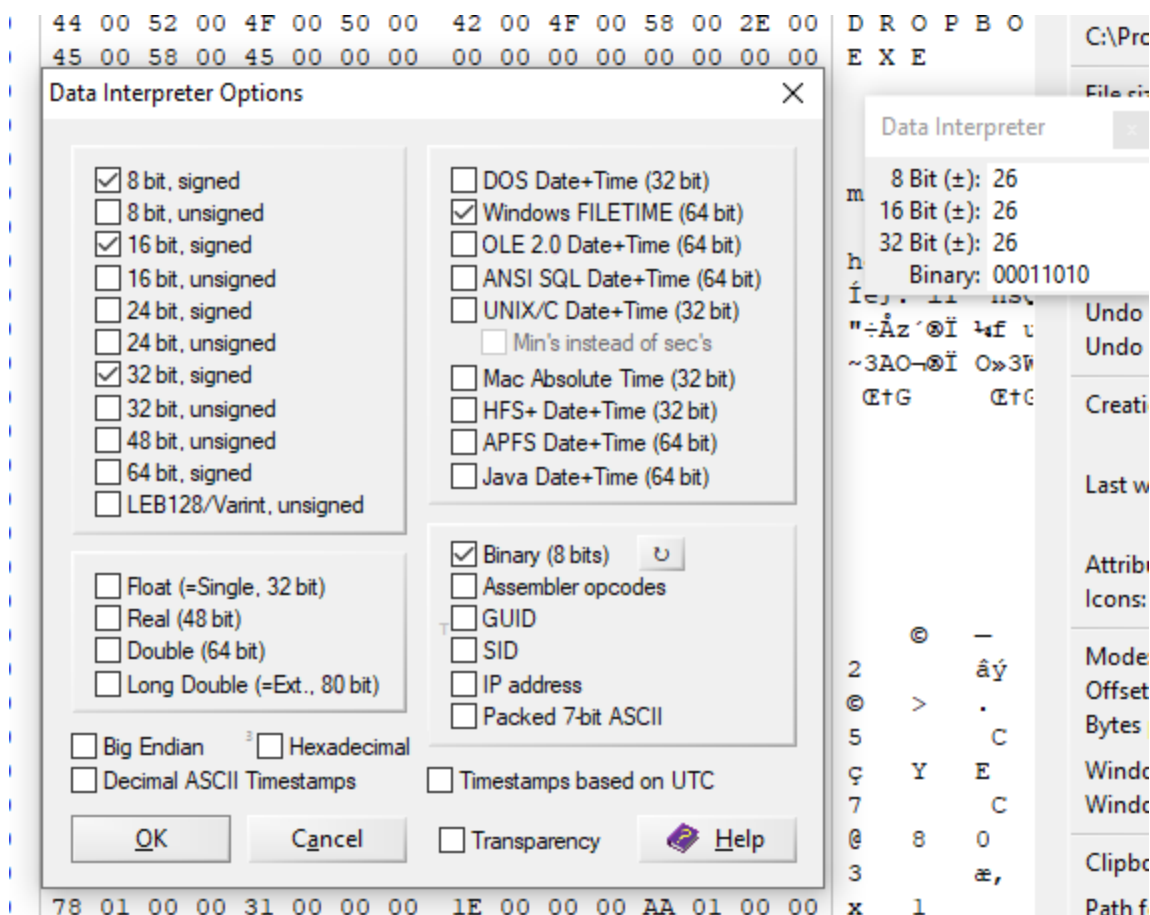


Step 3: Analyze Prefetch File

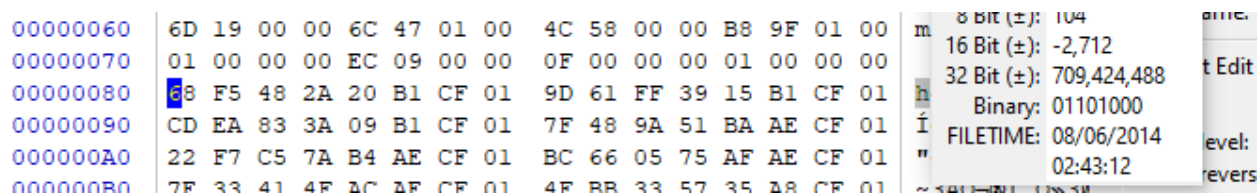
Ensure the Data Interpreter window is shown by going to View, Show, and check the Data Interpreter option.



Display the Windows Timestamp field in the Data Interpreter window by selecting Options, Data Interpreter, checking "Windows FILETIME (64 bit)" and pressing OK.



Go to Offset 0x80 and document the most recent runtime.



Go to Offset 0x88 and document the modification date.

00000030	00 00		00 00 00 00 00 00 00 00
00000040	00 00	Data Interpreter	00 00 00 00 12 81 3E AA
00000050	00 00		A9 00 00 00 50 16 00 00
00000060	6D 19	8 Bit (±): -99	4C 58 00 00 B8 9F 01 00
00000070	01 00	16 Bit (±): 24,989	0F 00 00 00 01 00 00 00
00000080	68 F5	32 Bit (±): 973,037,981	0D 61 FF 39 15 B1 CF 01
00000090	CD EA	Binary: 10011101	7F 48 9A 51 BA AE CF 01
000000A0	22 F7	FILETIME: 08/06/2014	BC 66 05 75 AF AE CF 01
000000B0	7E 33 41 4F AC AE CF 01	01:24:54	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

Go to offset 0xD0 and document the counter in DECIMAL format.

11

000000A0	22 F7 C5 7A B4 AE CF 01 BC 66 05 75 AF AE CF 01		
000000B0	7E 33 41 4F AC	Data Interpreter	3 57 35 A8 CF 01
000000C0	00 8C 86 47 00		6 47 00 00 00 00
000000D0	0B 00 00 00 05	8 Bit (±): 11	0 00 00 00 00 00
000000E0	00 00 00 00 00	16 Bit (±): 11	0 00 00 00 00 00
000000F0	00 00 00 00 00	32 Bit (±): 11	0 00 00 00 00 00
00000100	00 00 00 00 00	Binary: 00001011	0 00 00 00 00 00
00000110	00 00 00 00 00	FILETIME: 01/01/1601	0 00 00 00 00 00
00000120	00 00 00 00 00	00:35:47	0 00 00 00 00 00