Maria Valencia

Csc 153

Lab 13

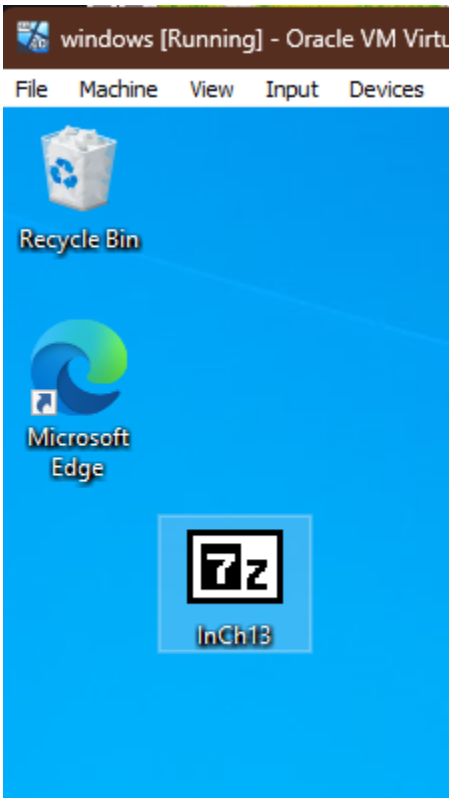
Cloud Forensics

Task 1 – Windows Prefetch Artifacts

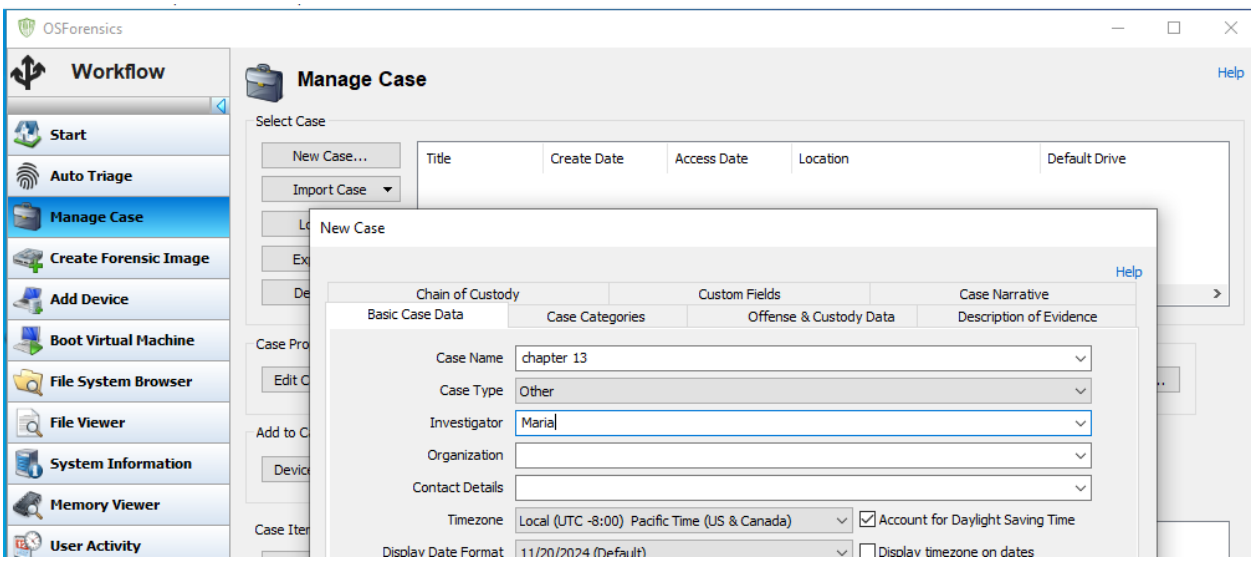
In this task you will find an application's MAC dates and counter using OSForensics and WinHex Data Interpreter in your Windows VM.

Step 1: Setup Case

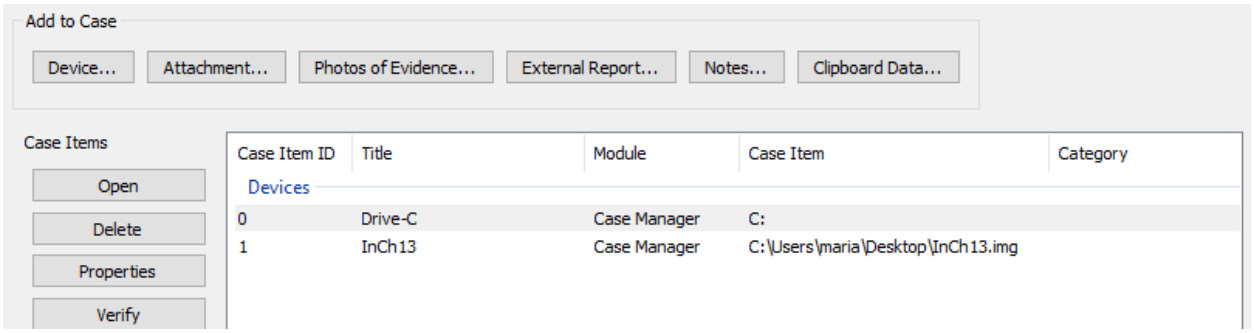
From your Windows VM, download the "InCh13.exe" to the machine. Run the EXE to extract the InCh13.img file.



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

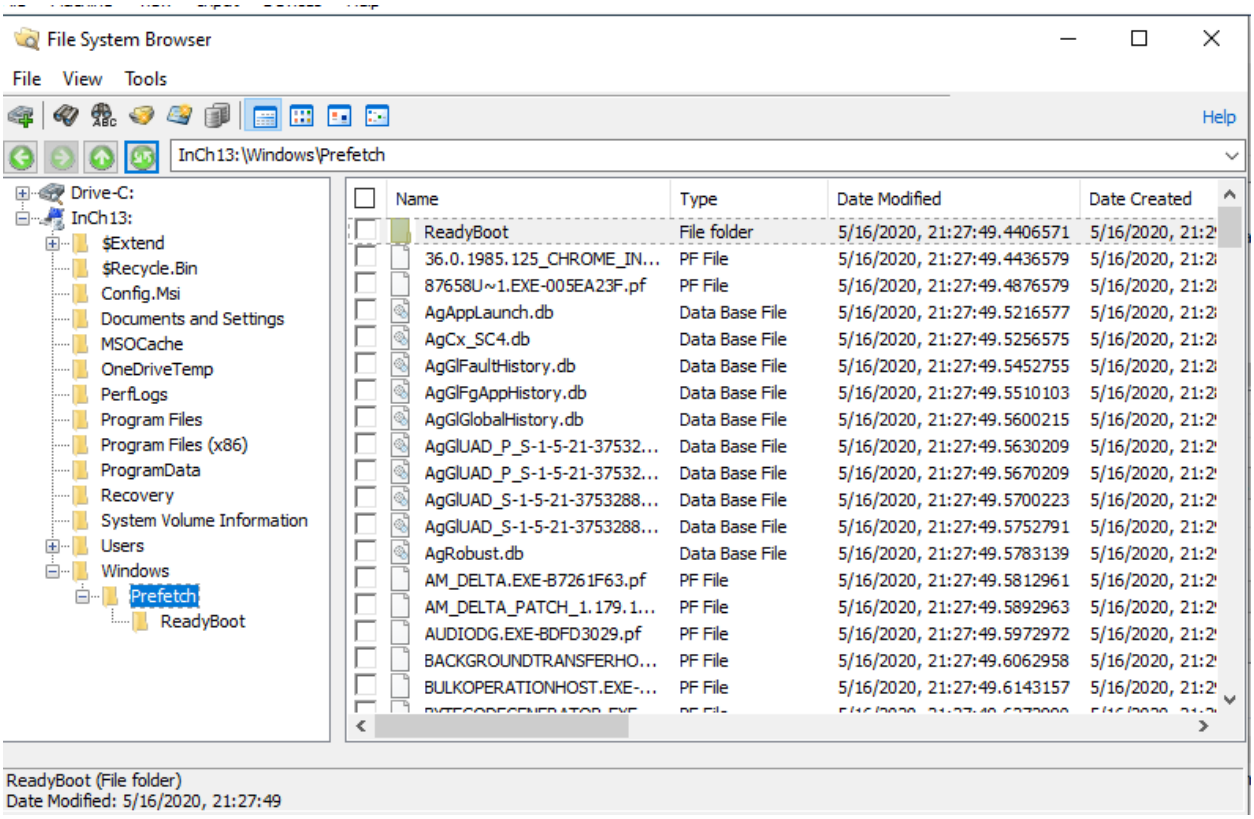


Add the "InCh13.img" as a device to the case using the "Device..." button. Select "Image File" and choose the path to your "InCh13.img" file.

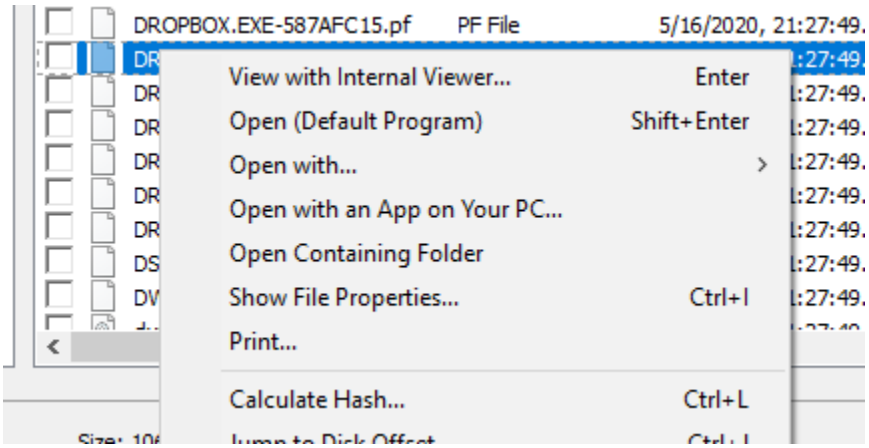


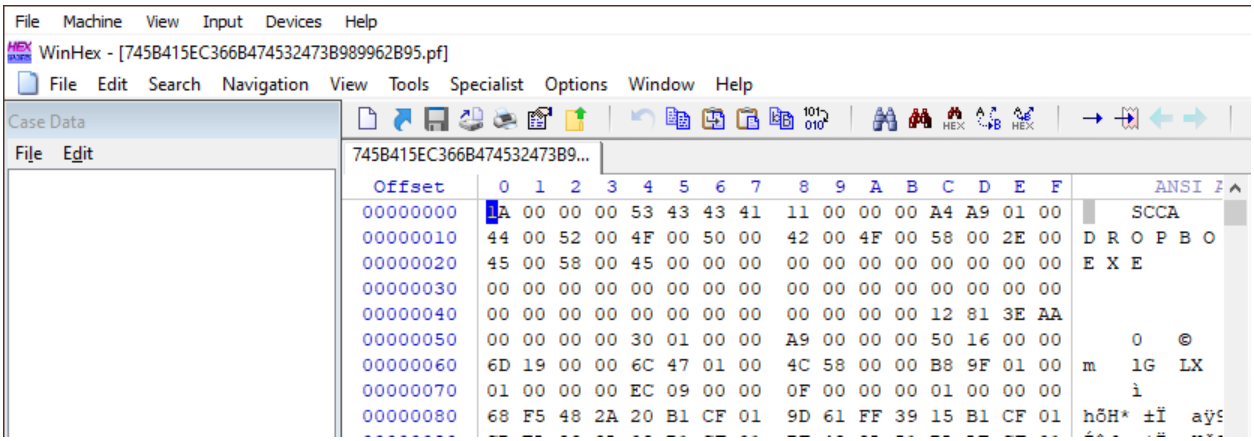
Step 2: Identify Target Prefetch File

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.



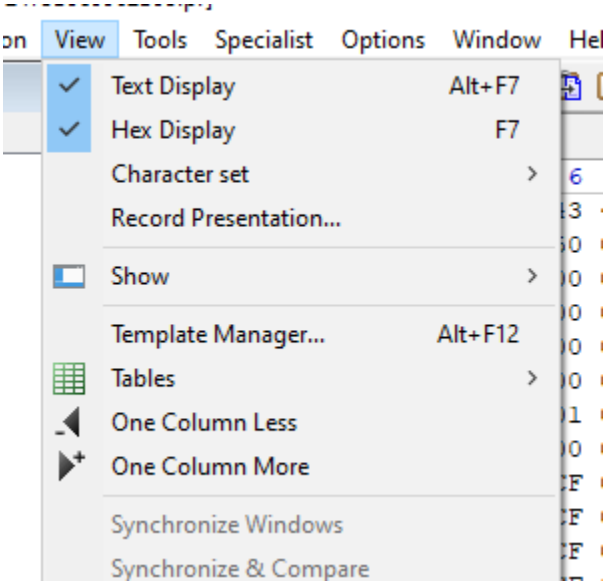
Scroll through the listings and find the "DROPBOX.EXE-AA3E8112.pf" file. Right click the file and choose "Open with..." and find the WinHex application (C:\Program Files\WinHex\winhex.exe".



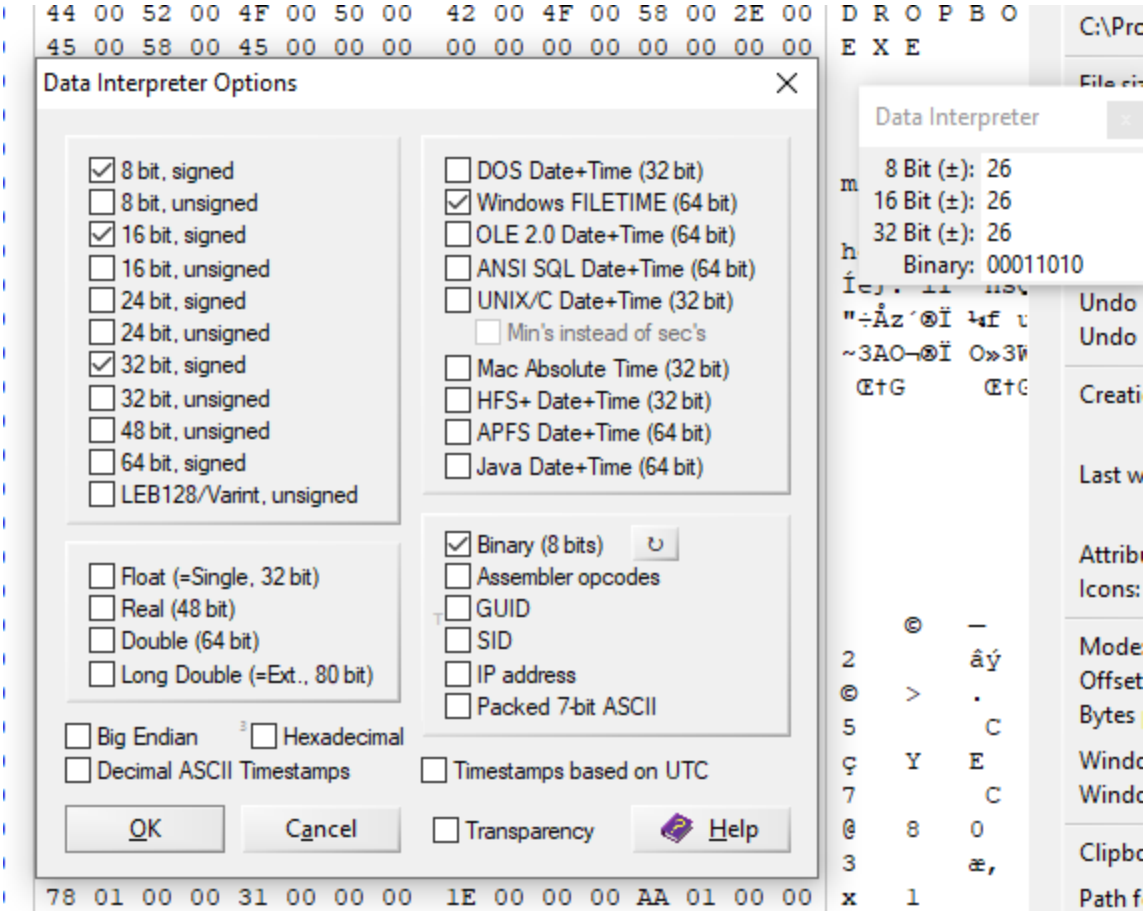


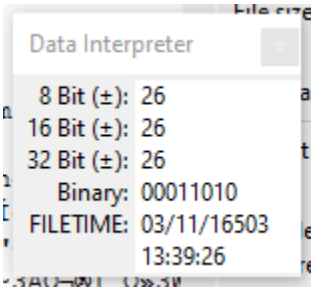
Step 3: Analyze Prefetch File

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

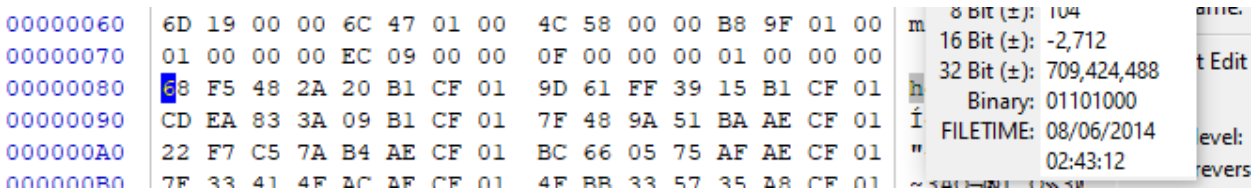


Display the Windows Timestamp field in the Data Interpreter window by selecting Options, Data Interpreter, checking "Windows FILETIME (64 bit)" and pressing OK.

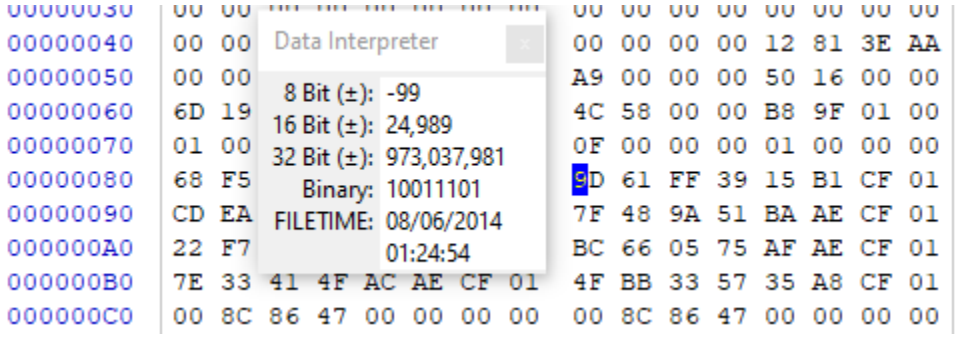




Go to Offset 0x80 and document the most recent runtime.



Go to Offset 0x88 and document the modification date.



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

11