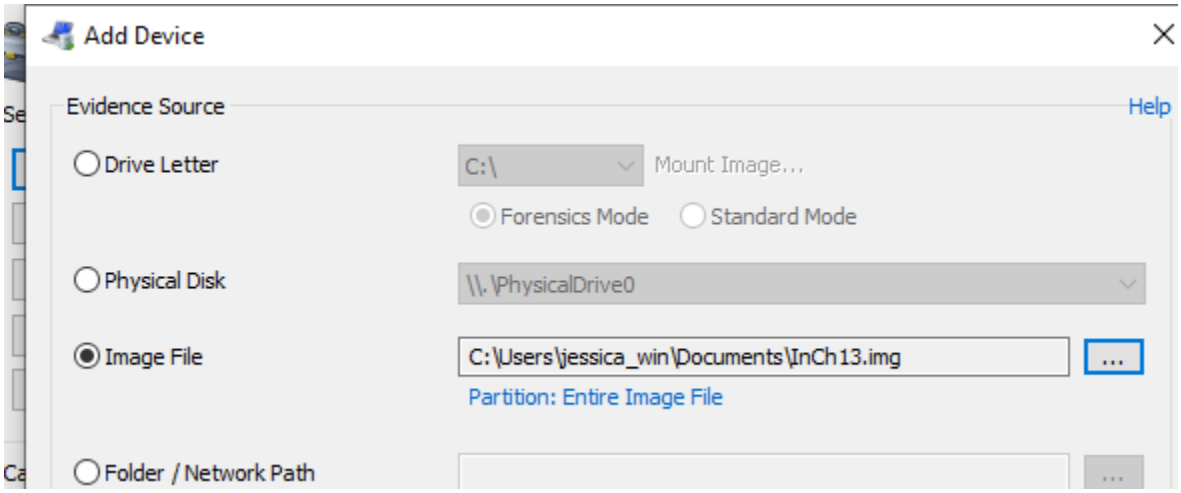
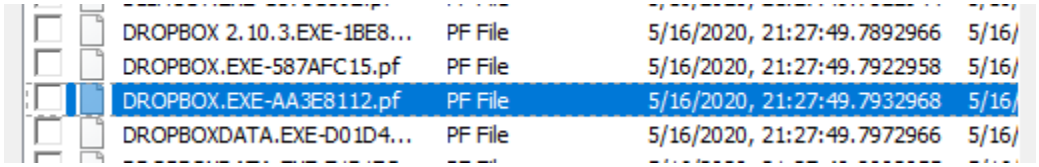
Task 1: Windows Prefetch Artifacts

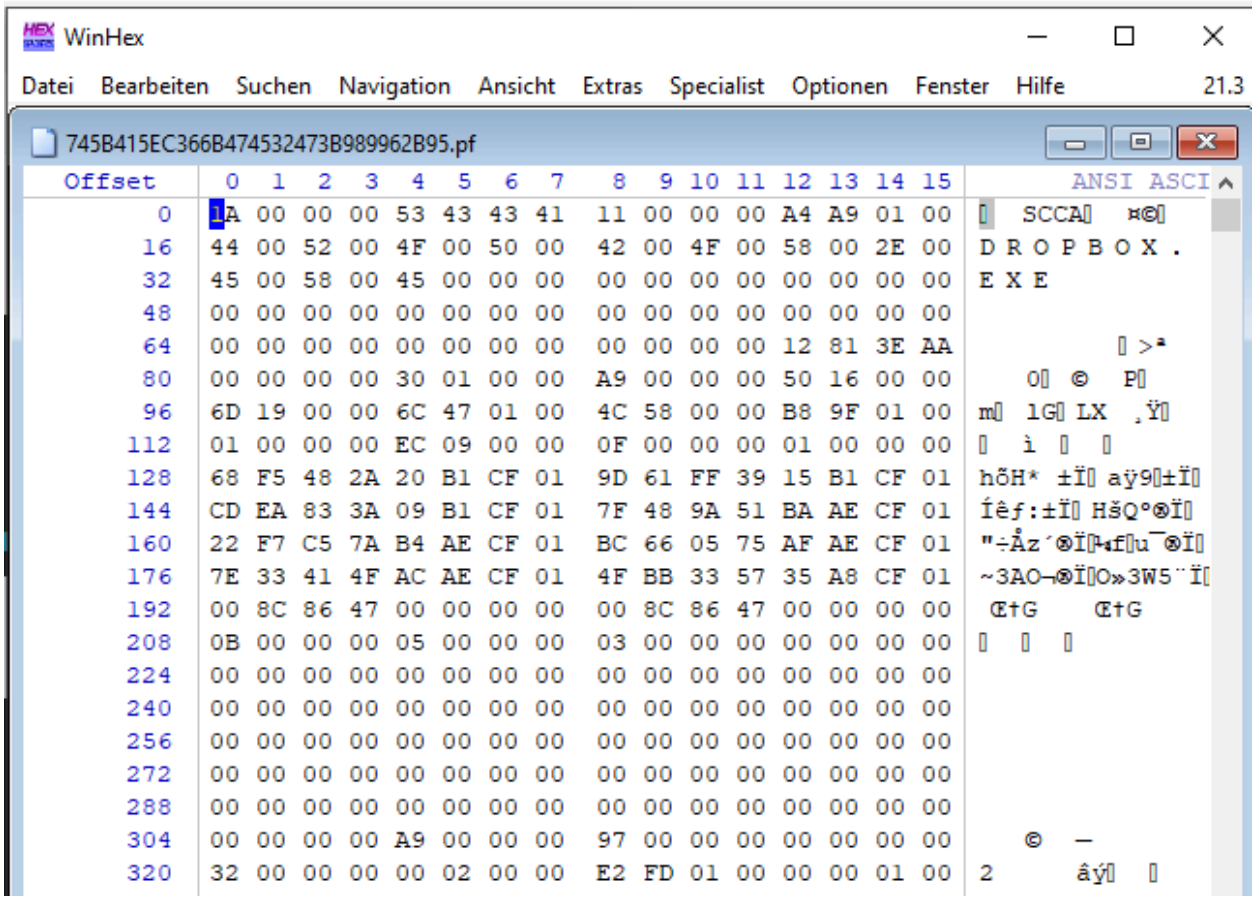
Step 1: Setup Case



Successfully created new case with given image file.

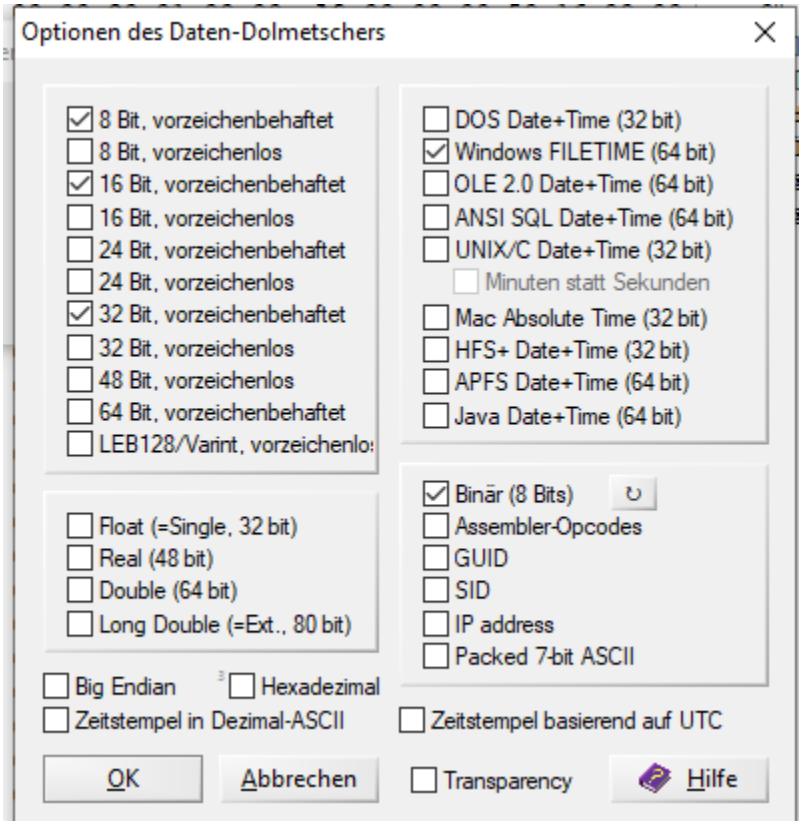
Step 2: Identify Target Prefetch File



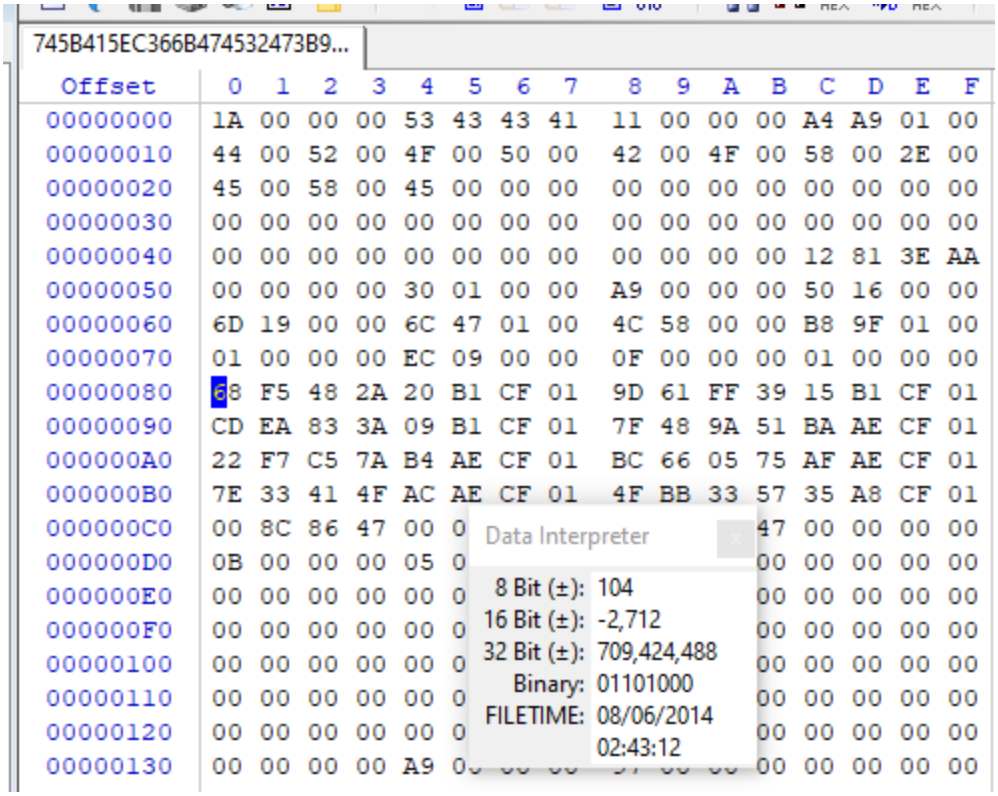


Successfully found target file and opened the .pf file in WinHex.

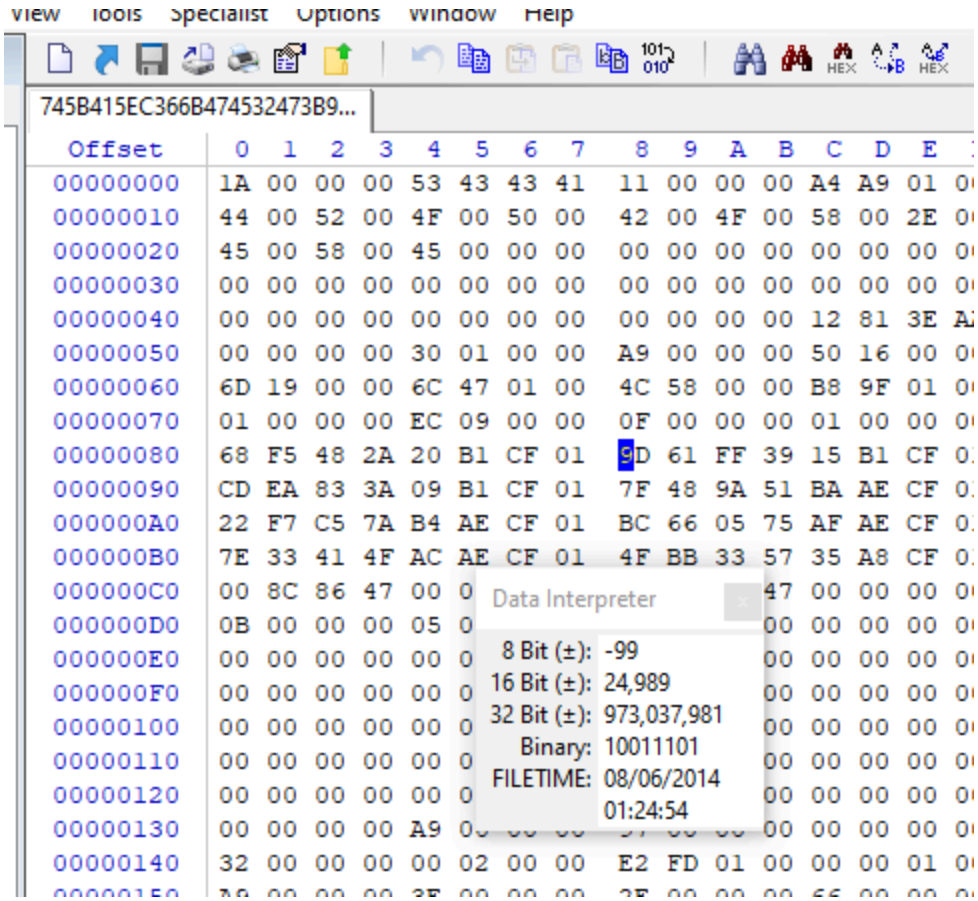
Step 3: Analyze Prefetch File



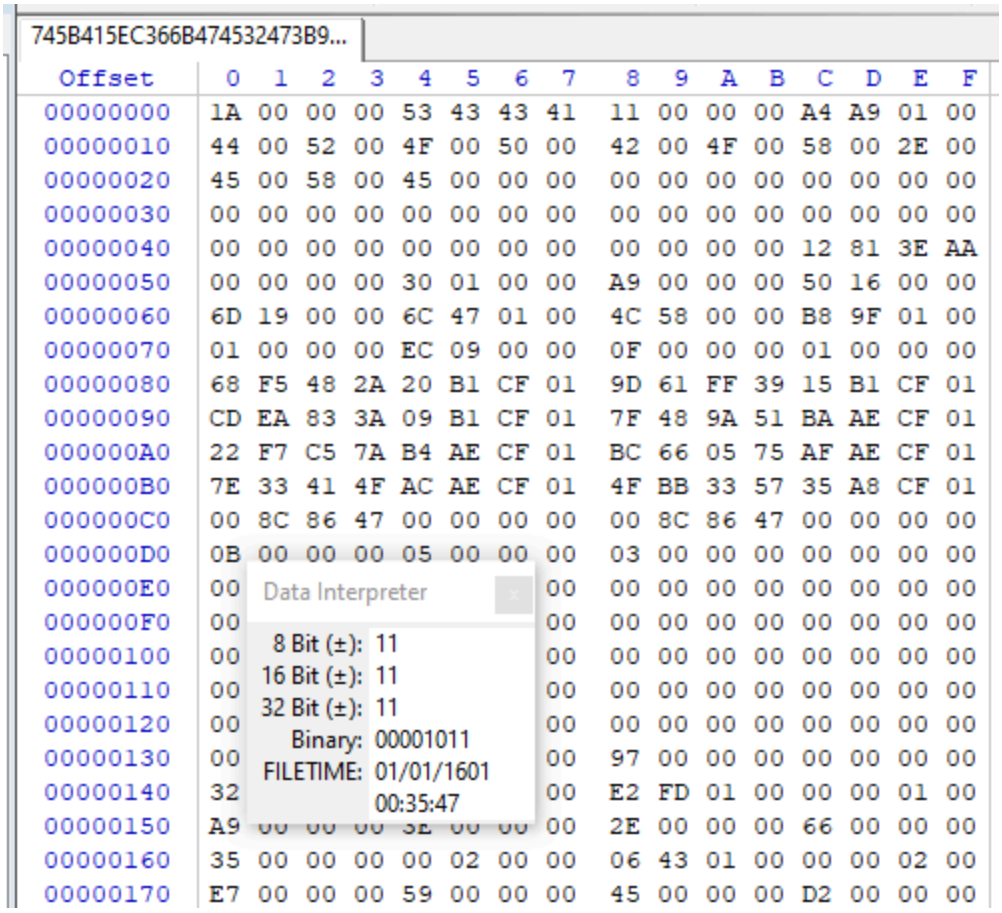
Not sure why my WinHex is in a different language, but I managed to follow the pictures and was able to apply the same settings.



Documented the runtime at offset 0x80.



Documented offset 0x88.



Documented offset at 0xD0 (208).