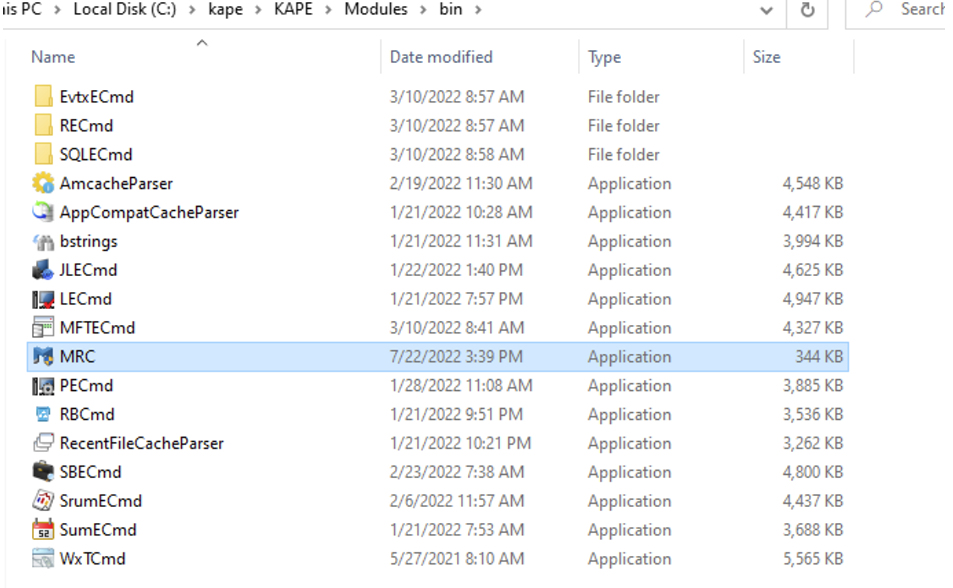
**Capturing Memory with KAPE**

The first step to capturing memory with KAPE is adding the [Magnet Forensics RAM Capture](https://www.magnetforensics.com/resources/magnet-ram-capture/) tool (~350kb) to the KAPE’s modules\bin folder. A copy of the RAM capture tool can be obtained below. If downloading directly from the Magnet site, make sure to rename the binary as MRC.exe as KAPE will look for that exact file name in the bin folder.



Once the tool is in the KAPE repository and sent to the customer, the customer should run KAPE with the following parameters:

.\kape.exe --tsource C: --tdest C:\kape\_data --tflush --target !SANS\_Triage --msource C:\ --mdest C:\kape\_data\memory --module MagnetForensics\_RAMCapture

These parameters tell KAPE to clear the C:\kape\_data folder, and then write the outputs of the SANS\_Triage artifact collection suite to C:\kape\_data as well as the memory dump into C:\kape\_data\memory.

The memory output should be a .raw format dissectible by Volatility. It’s a good idea to have the customer take note of the OS build as newer operating systems (builds > Win10x64\_19041) might not be supported on Volatility 2, and should be examined with Volatility 3.