Memory capture for Windows OS

Note: We will first acquire live memory (RAM) from a Windows system based on the concept of "Order of Volatility" which states that more volatile data must be acquired before acquiring other data that may be less volatile. Live memory of a system i.e. the RAM is more volatile than the data on the hard disk(s) so it must be acquired first.

1 Preparation (on standalone machine)

1. "Magnet RAM Capture" a free imaging tool designed to capture the physical memory of a suspect's computer, allowing investigators to recover and analyze valuable artifacts that are often only found in memory. A portable version of this may be downloaded from: https://www.magnetforensics.com/resources/magnet-ram-capture/

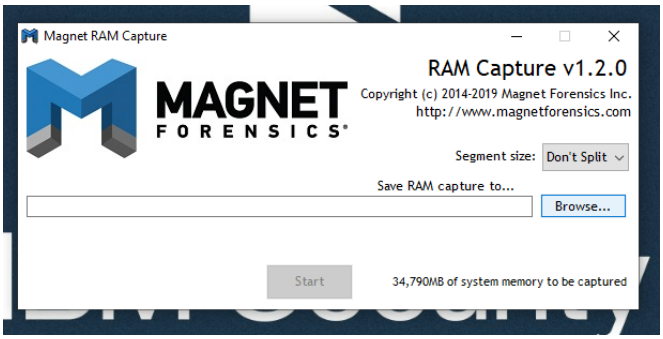
2. Ensure that you have compression software capable of creating encrypted ZIP archives available in your system. If not, IBM X-Force IRIS recommends using 7-Zip Portable, available from official website: http://portableapps.com/apps/utilities/7-zip_portable or any other tool of your choice.

3. Prepare storage media, with at least the same size as media in target machine. Tool allows forensic images to be stored on external hard drive attached to target machine. Perform a quick format of a storage media with NFTS file system – all data on this media may be irrecoverably lost! If it is not possible to use external storage media, network shared can be used as an alternative.

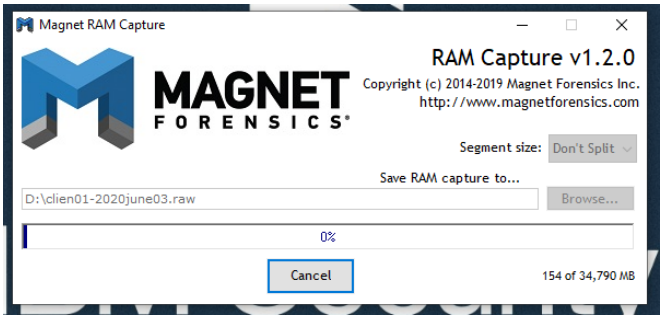
4. Copy "MRCvXXX.exe" and if necessary "7zip Portable" onto the media.

2 Acquiring live Memory (on target machine)

1. Execute Magnet RAM Capture icon to start the program.
2. In Magnet RAM Capture, select **Browse** → **<External Device Directory of Capture Output>** …
3. Select destination path for the memory image file. This should be a folder in the external media connected to the target Windows system. Also select a memory dump file name following the pattern <hostname-date> (i.e. clien01-2018mar03).



4. Click **"Start"** button on the same screen to begin the live memory acquisition process.



5. At the end of the process you will have the memory dump file created in the desired folder on the external media.