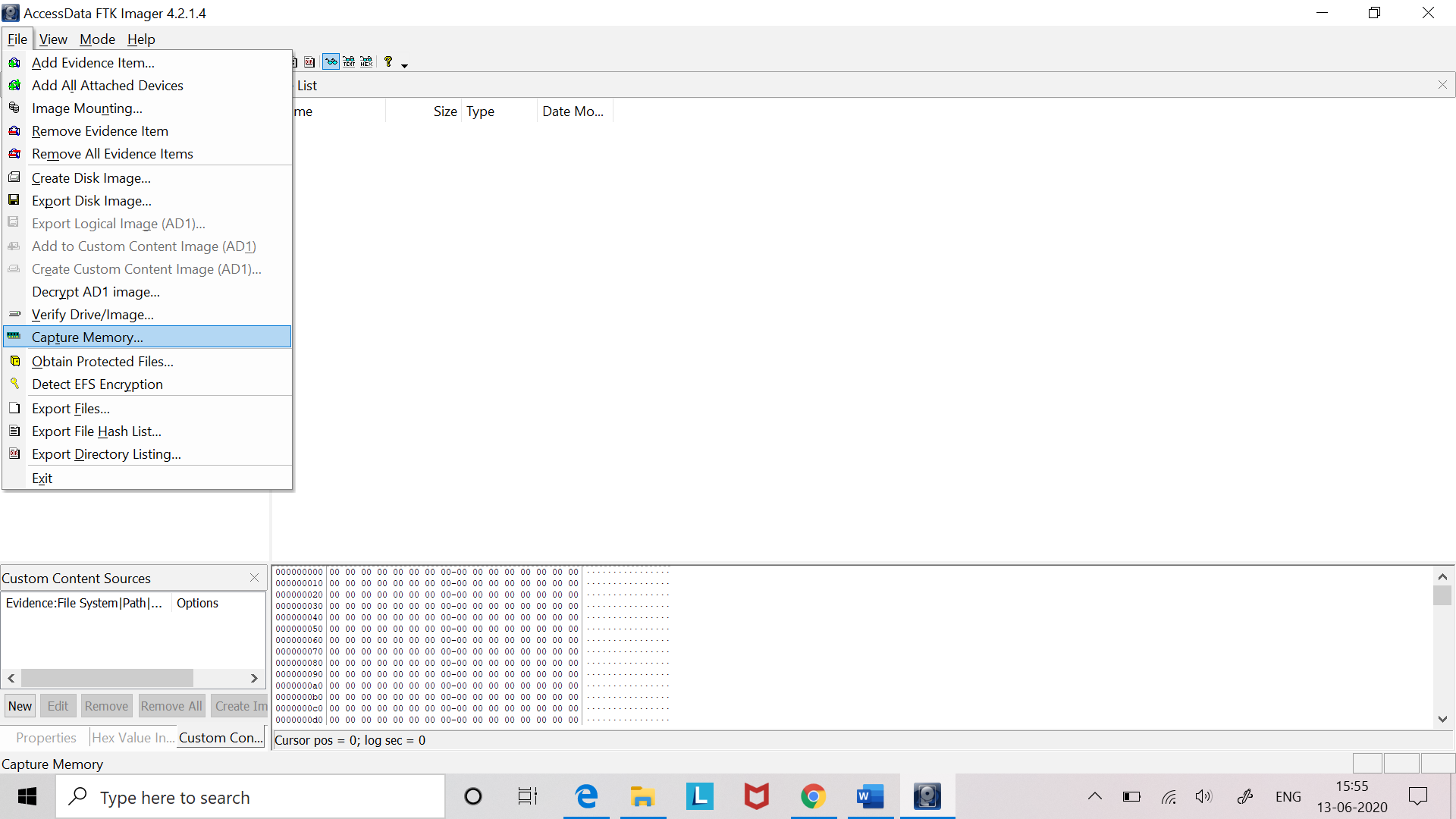
Capturing live memory (RAM)

FTK Imager provides us the facility to capture the live memory i.e. RAM. It is useful when an investigator found a running computer. So, before shutting down the computer an investigator can capture RAM. This memory can contain valuable forensics data about the current state of the system. It can contain useful evidence to proceed in the investigation.

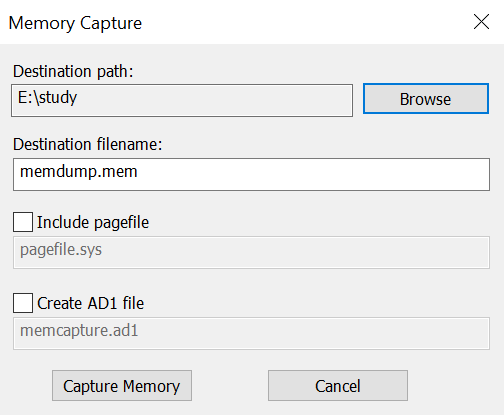
We can start capturing RAM memory by one of the following methods:

* File >> Capture Memory

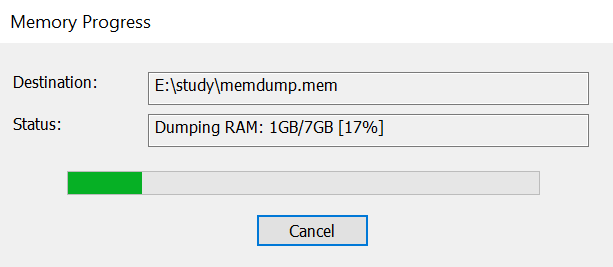


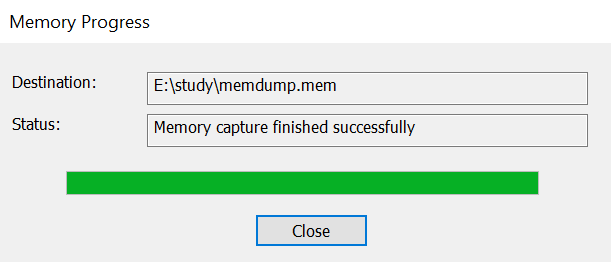
* Using capture memory icon  from the toolbar.

Choose the destination folder to save the memory dump (image of live memory). Start capturing the memory by clicking the **Capture Memory** button.



It will take few seconds to capture memory. Image file will be saved at the specified folder.







We can analyse this memory dump by using **Tool Volatility**. It will open the memory dump and displays the processes that were running at the time of memory capture. We can analyse those processes individually and find out the malicious processes and many more.