Memory acquisition process is one of digital forensics act. There are several tools that support memory acquisition process. At this time, there is a feature named secure mode that can caused crash or error in memory acquisition tools system and caused the tools to be unusable, also the loss of the computer memory. This study is experimenting to find the effect on memory acquisition tools performance while running in secure mode. After getting the experiment results, the analysis is going to be carried out towards memory acquisition tools using static code analysis, which is one of the techniques of reverse engineering, using IDA. This study aims to find any kind of occurrences that happen on memory acquisition process while in secure mode and find the cause of it. The purpose of this study is to be useful for digital forensic tester in understanding the potential risk of the secure mode impact in acquisition process. The experiment shows that Autopsy version 4.7 cannot run properly in VSM environment, different with FTK Imager. The results from the analysis define that the difference between library on normal kernel and secure kernel is the one that caused the program to terminate while in secure mode. In advance, the operating system that runs in the device are the other reasons of memory acquisition tools cannot run properly on VSM environment. It is caused by the difference in security features that is being provided by a specific operating system.