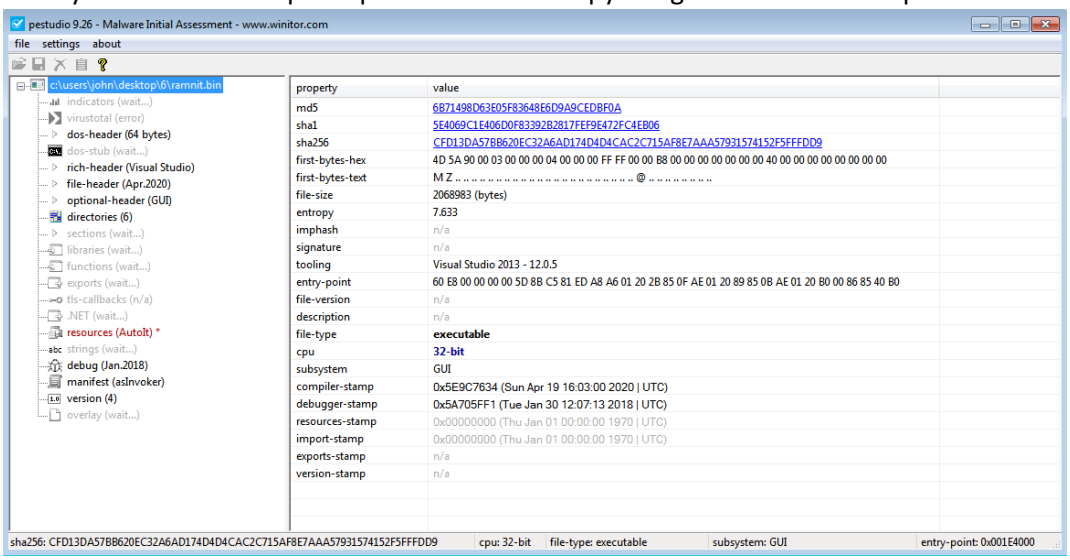
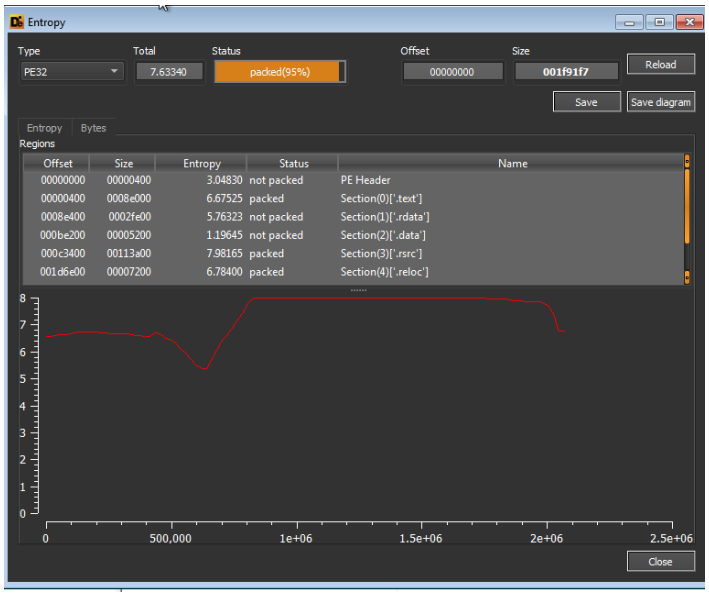
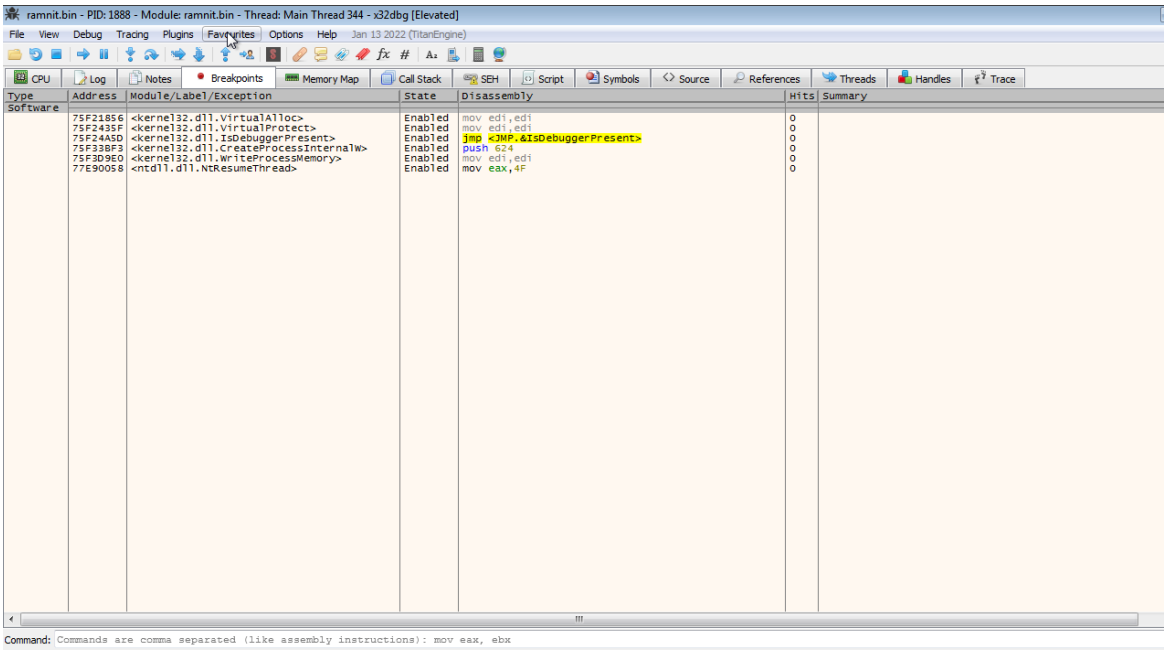
Initally we load the sample in pestudio and entropy is high which show it is packed.



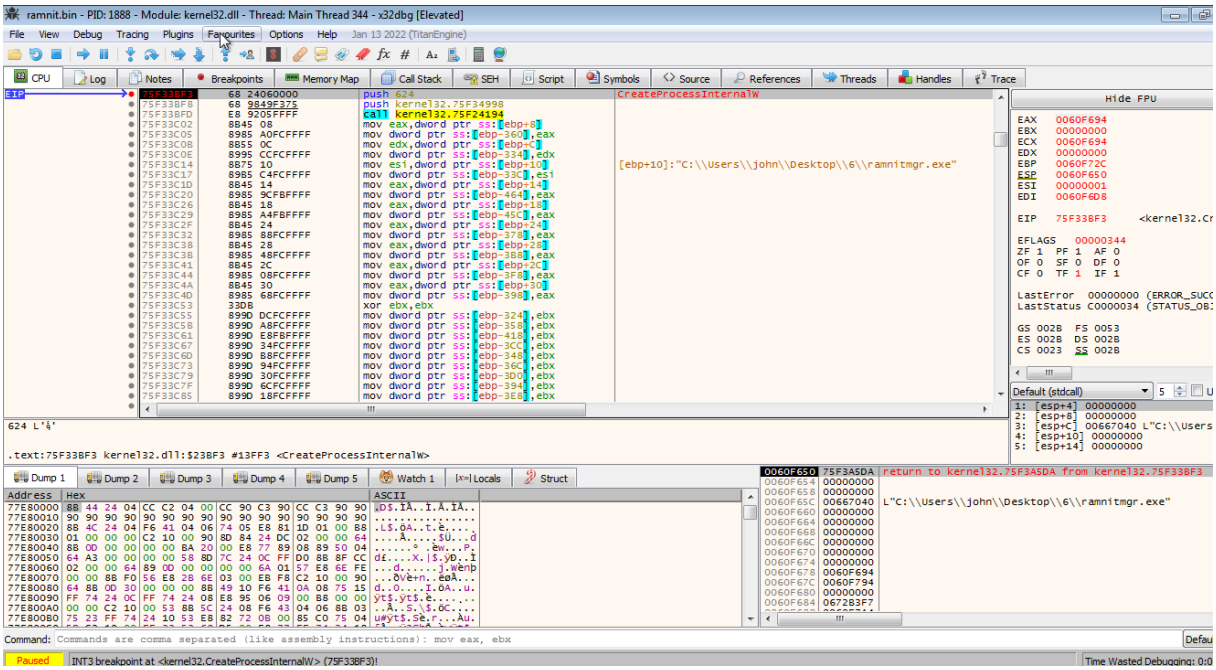
Now we loaded the sample in DetectItEasy and view the entropy i.e.7.63 and it is showing the sample status as packed.



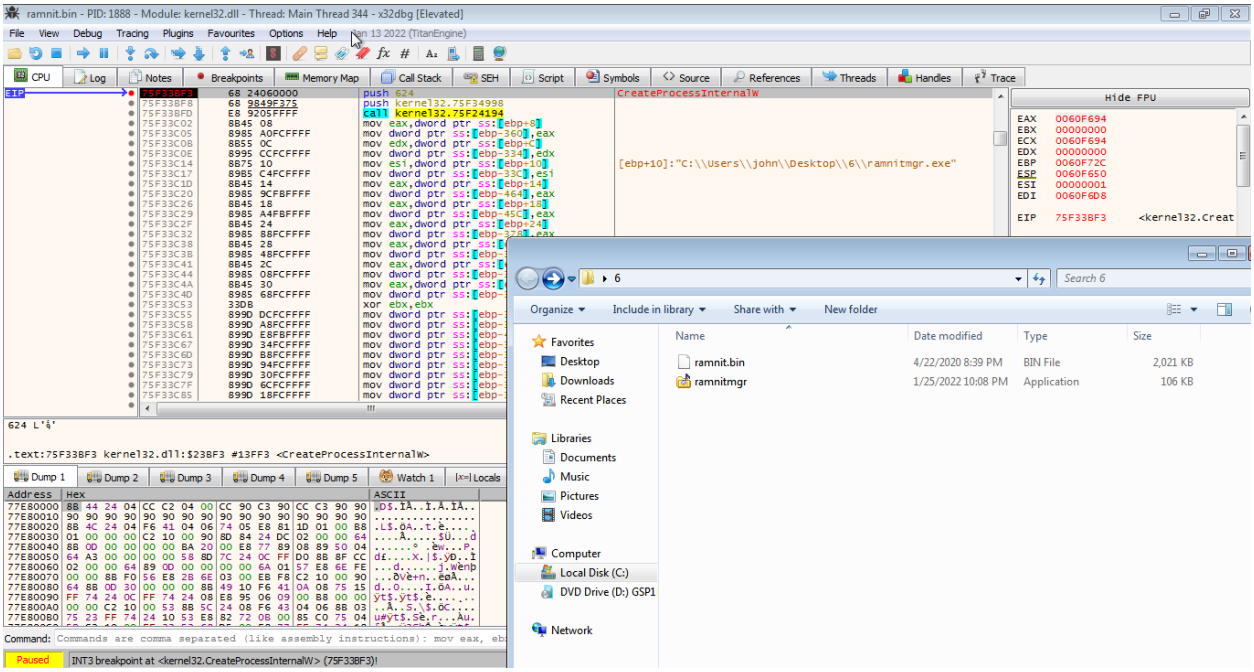
Now we will load the sample in x32dbg and put breakpoint on VirtualAlloc, VirtualProtect, IsDebuggerPresent, CreateProcessInternalW, WriteProcessMemory, NtResumeThread.



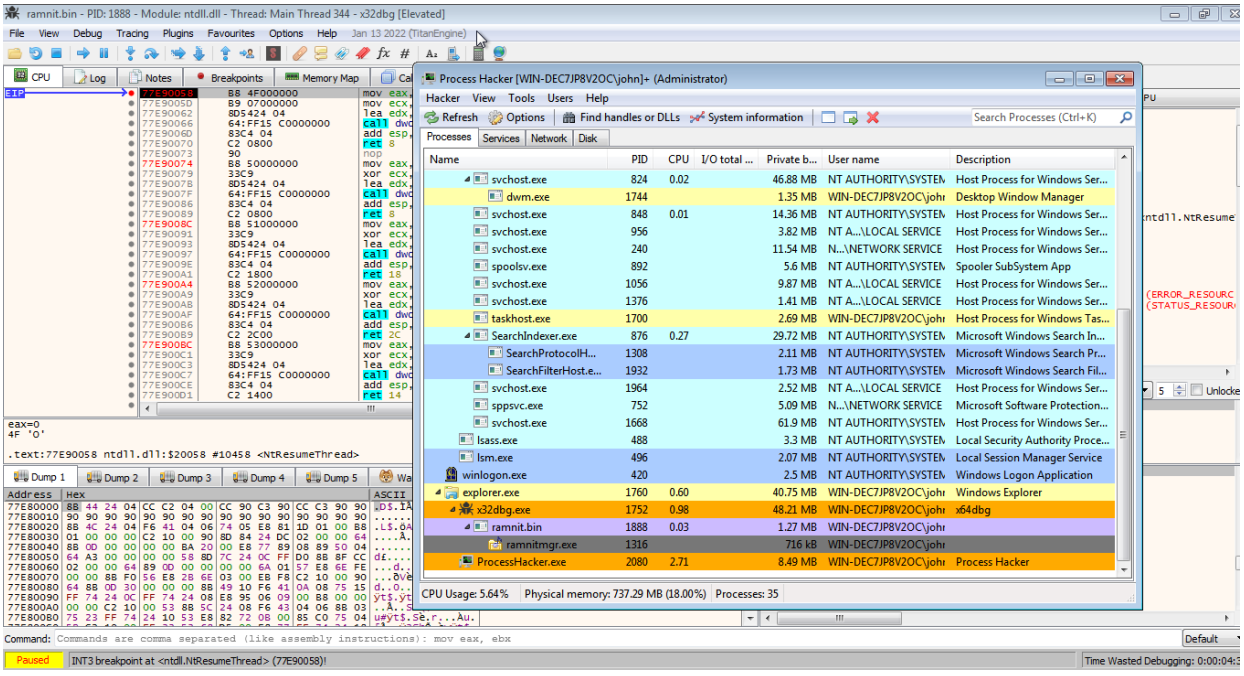
Now we hit the CreateProcessInternalW it will run the file ramnitngr.exe which is just dropped.



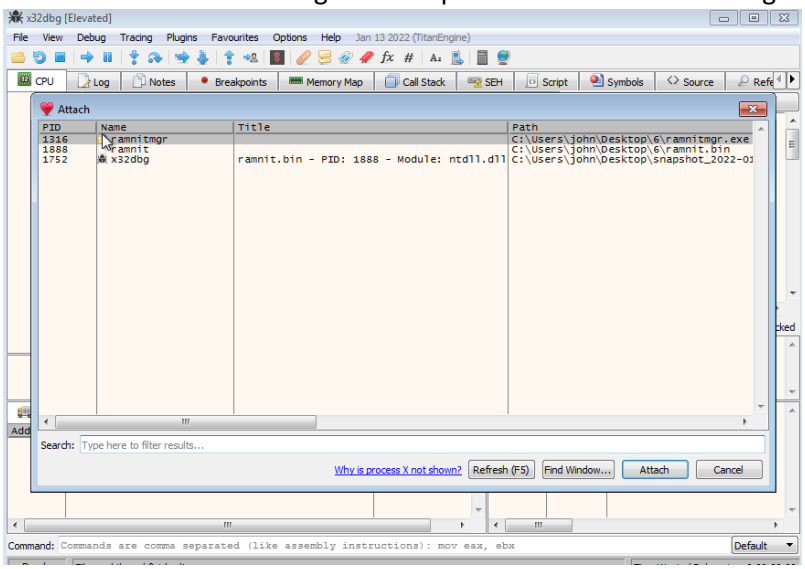
Here is the dropped file, Now to run this API we will click on “run to user” code, we can verify it using the process hacker.



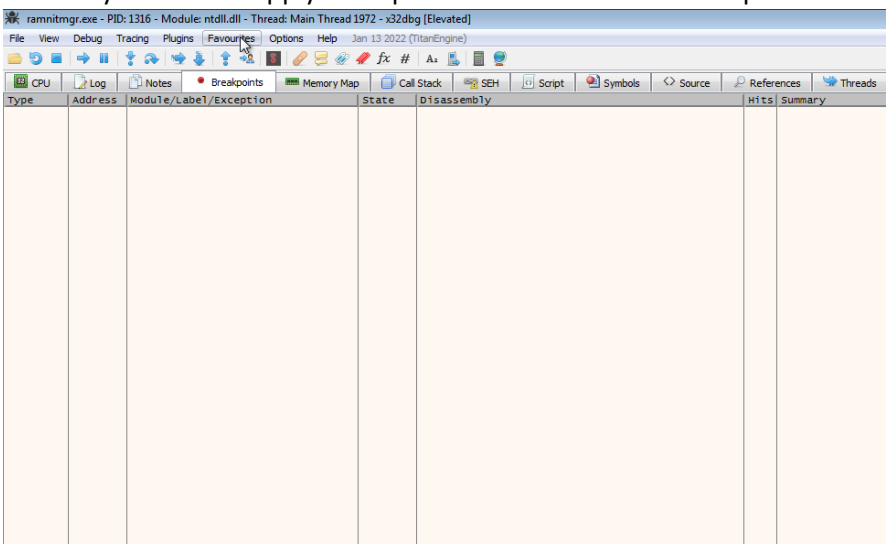
Here we can see ramnit had spawn the new process ramnitmgr.exe using API CreateProcessInternalW .



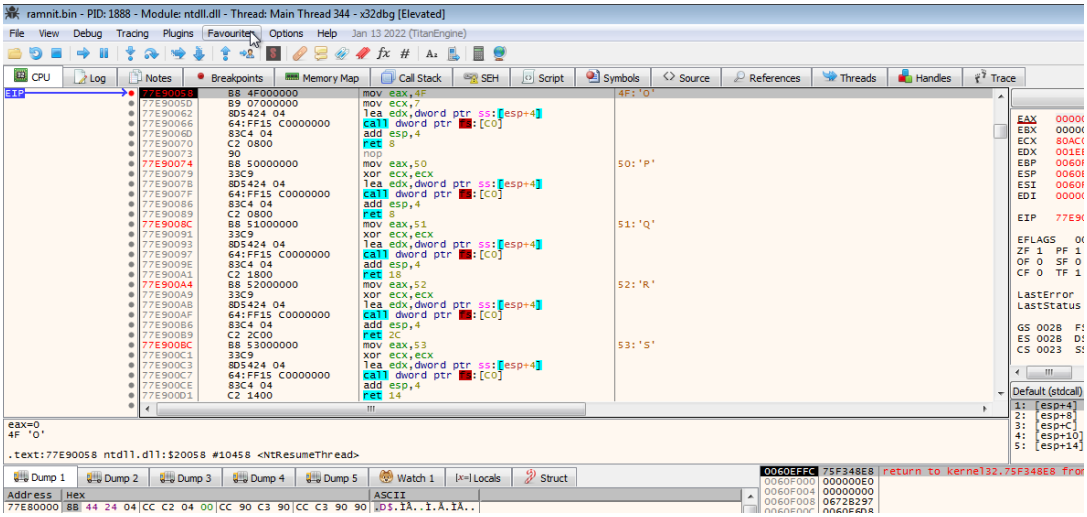
Since we know it is running we will open new instance of x32dbg and attach it.



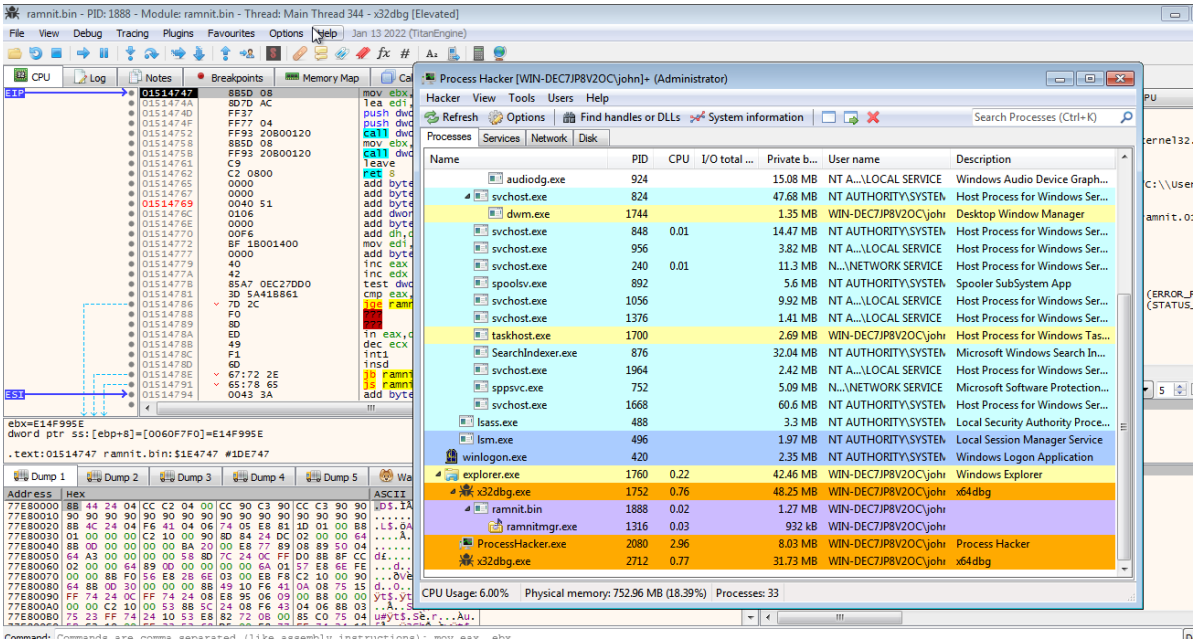
Currently we cannot apply breakpoints here because the new process is currently in suspended state.



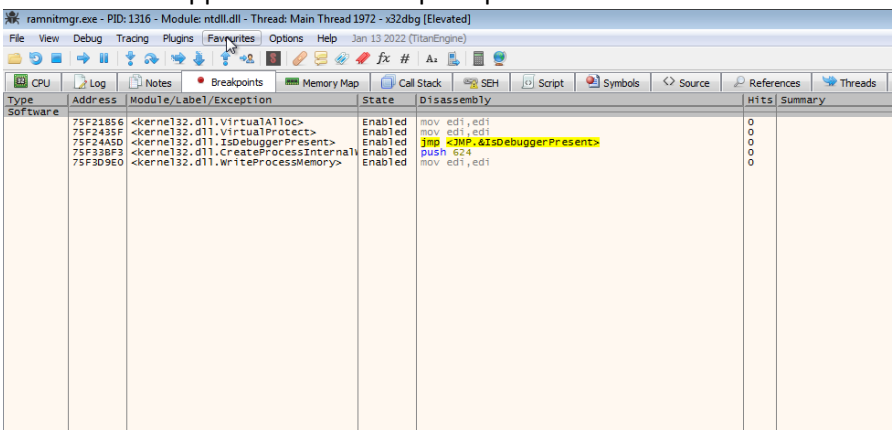
Now here switch to the initally loaded sample and clicked the “run to user code” this make the API to run and after that we can apply the breakpoints.



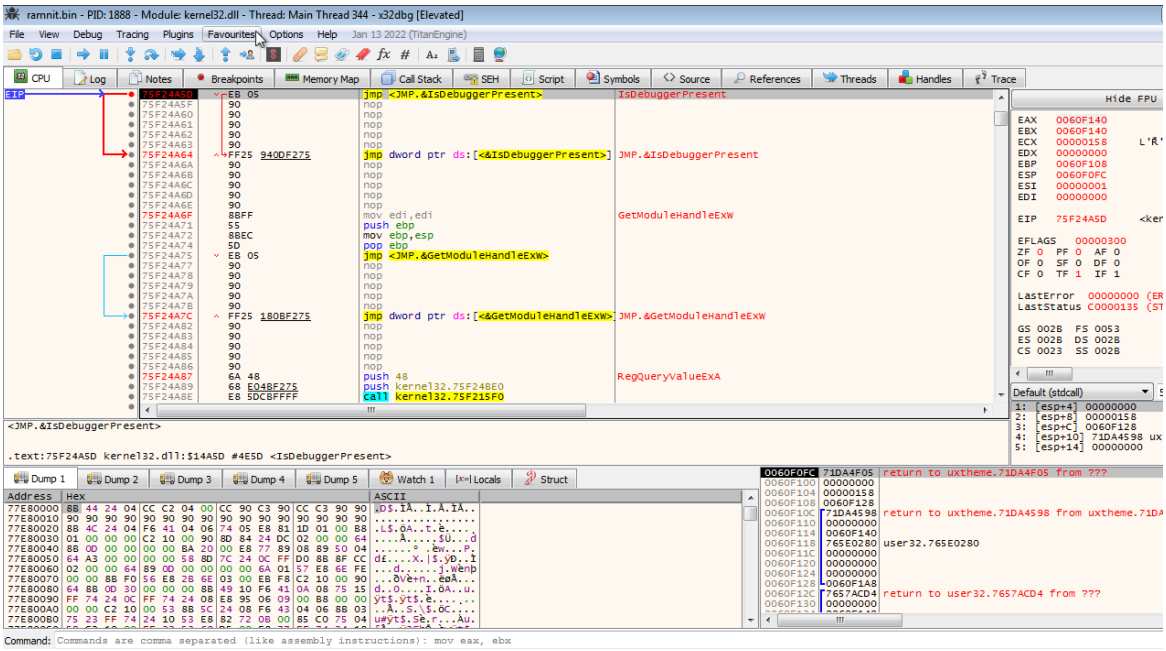
Here we can see in Process Hacker it is now in running state.



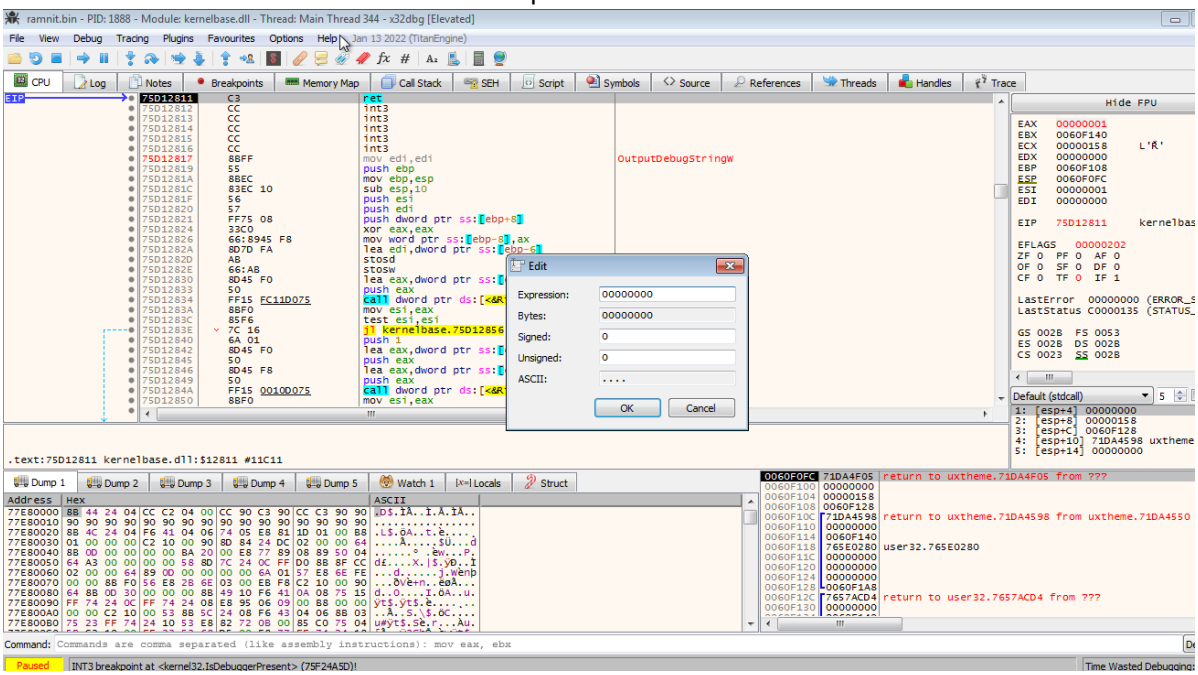
Here we have applied all the breakpints press f9.



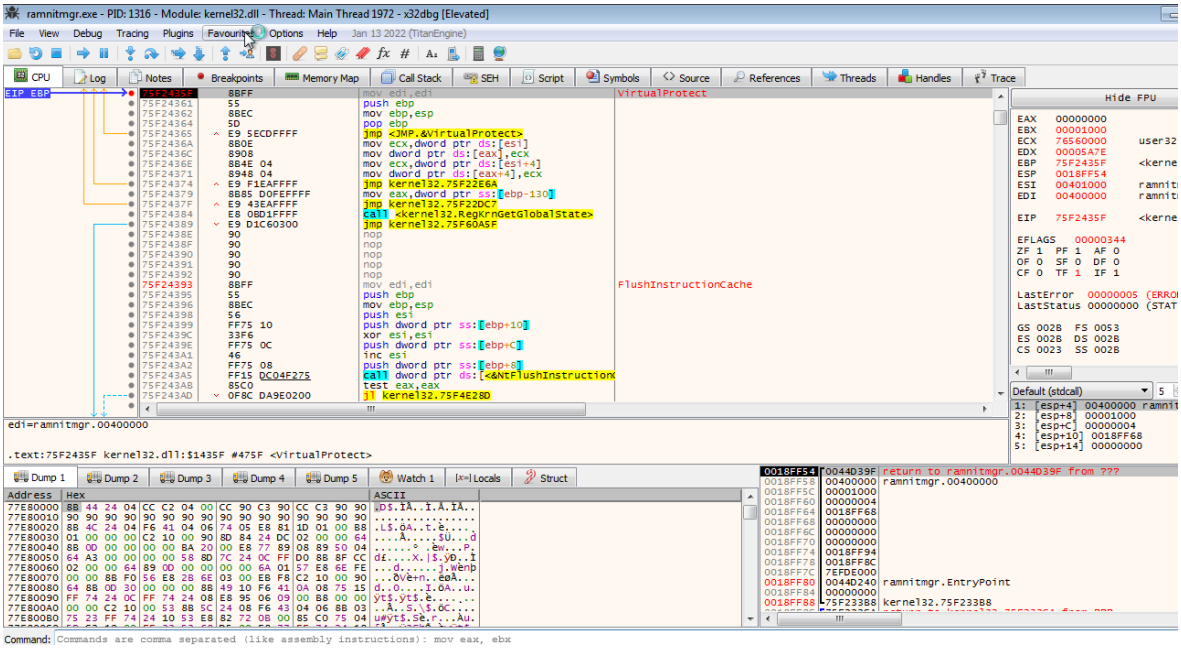
Now we hit the IsDebuggerPresent press the “execute till return ” and modify the value returned in eax to 0.



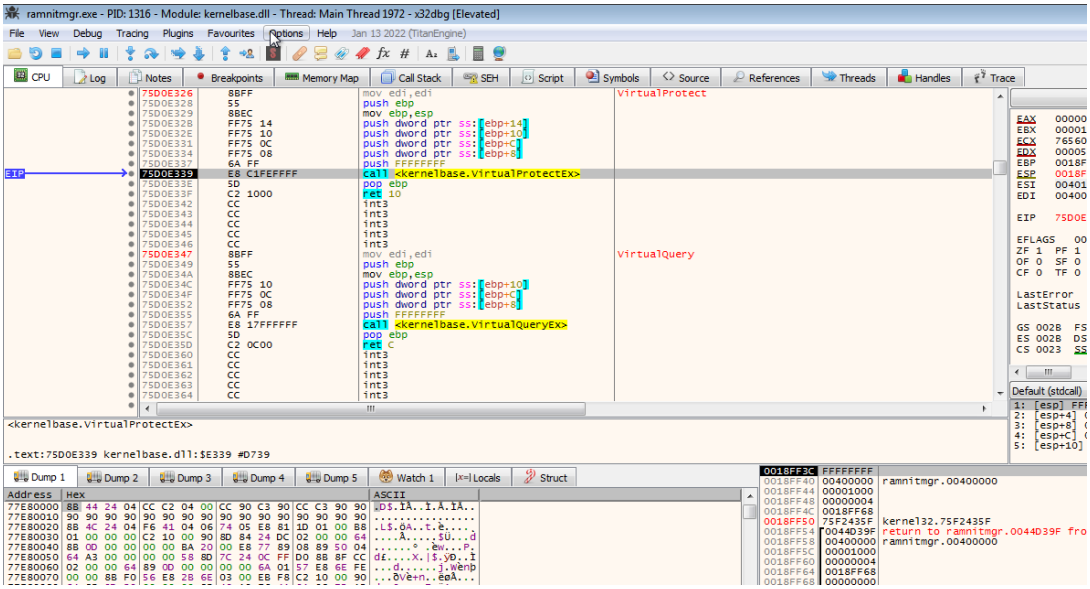
Here we modified the return value to 0 and press f9 it will continue to run.



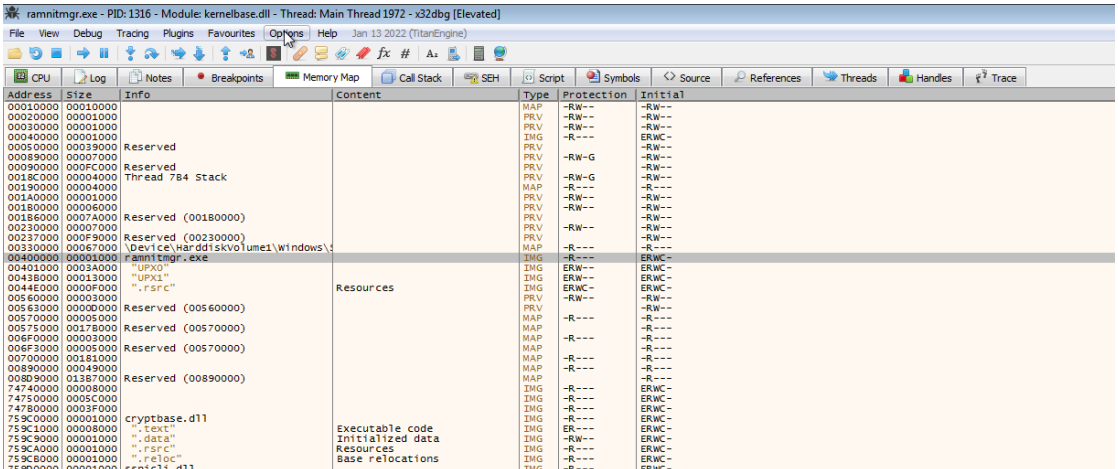
Now again we switch to the ramnitmgr.exe and here we hit the breakpoint at VirtualProtect.



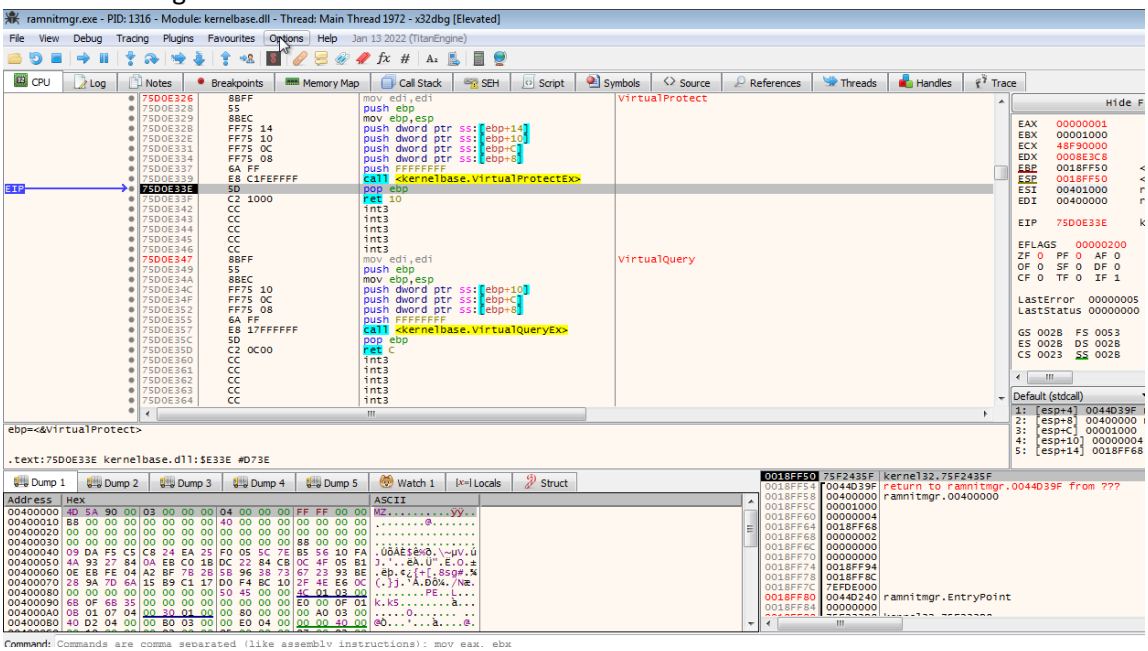
Now here look at the second parameter that is the location of memory where it wants to change the permission bits and dump that location into dump1.



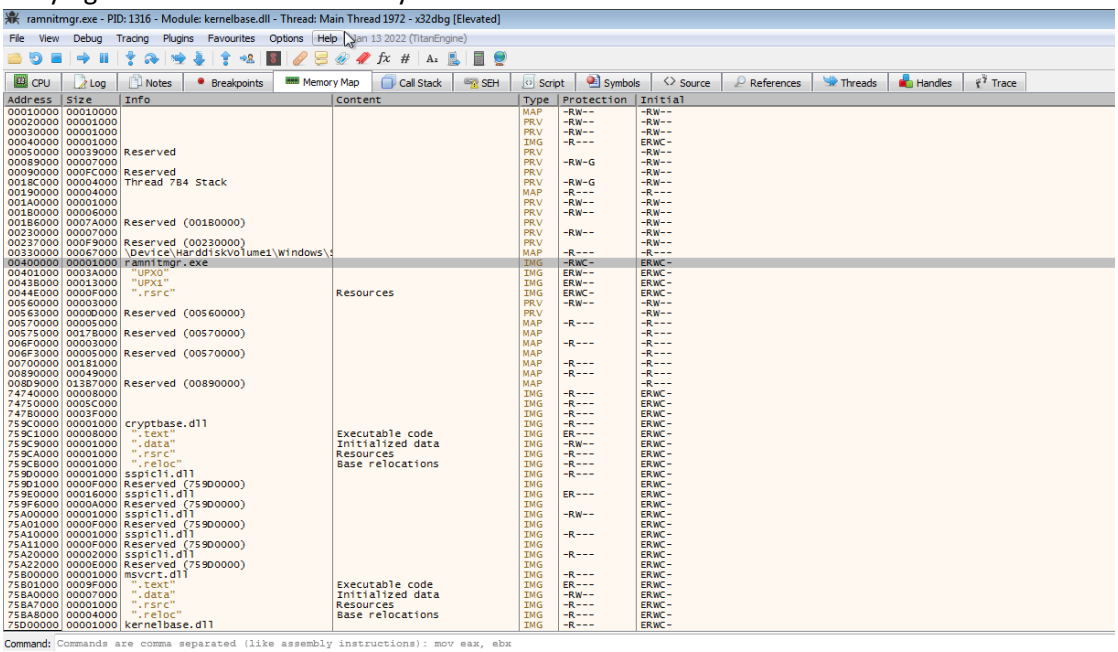
Now here view that memory location at Memory Map at this moment it is read only.



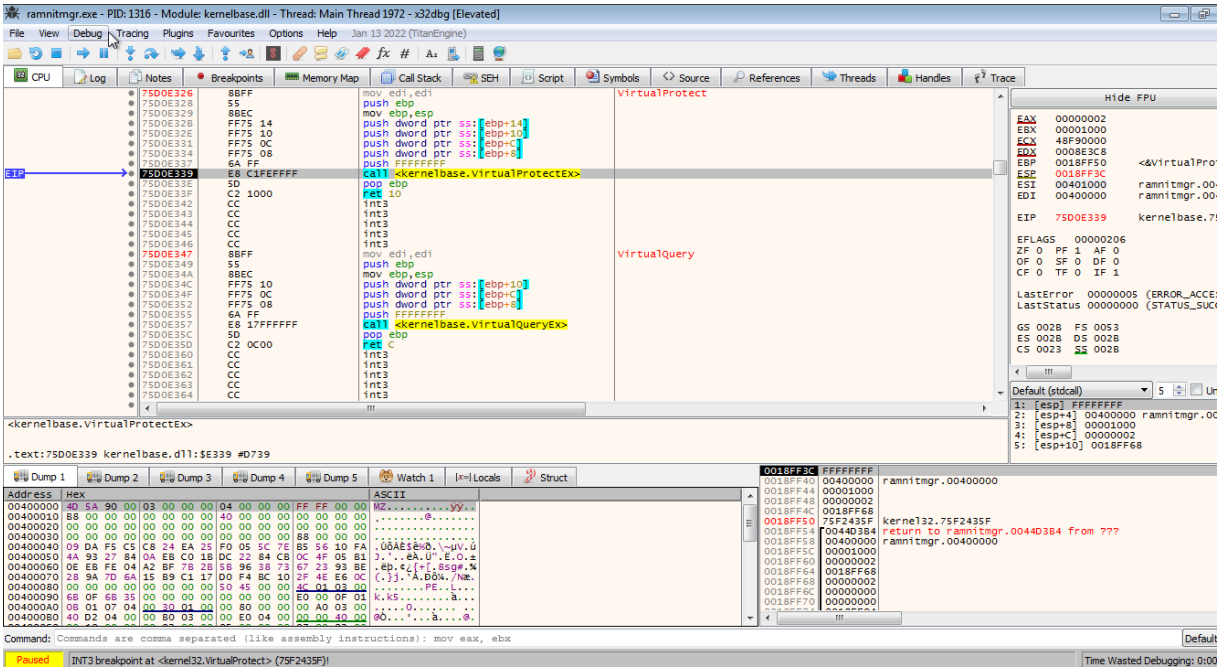
After executing the call.



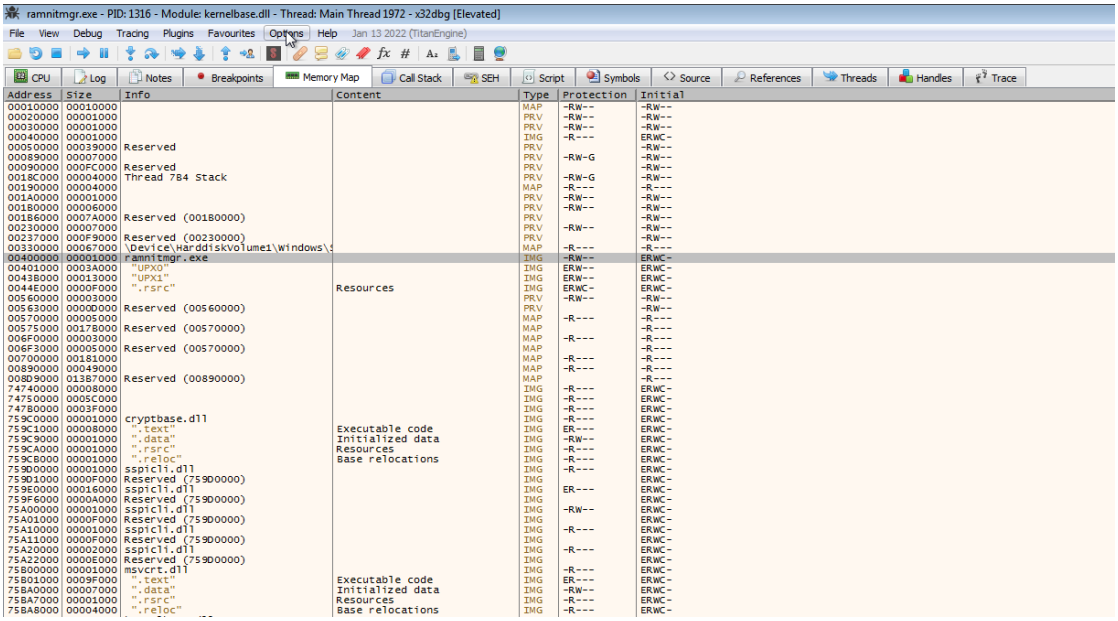
We noted now that permission for that region has been changed to read write here we can know that it is trying to write into this memory location.



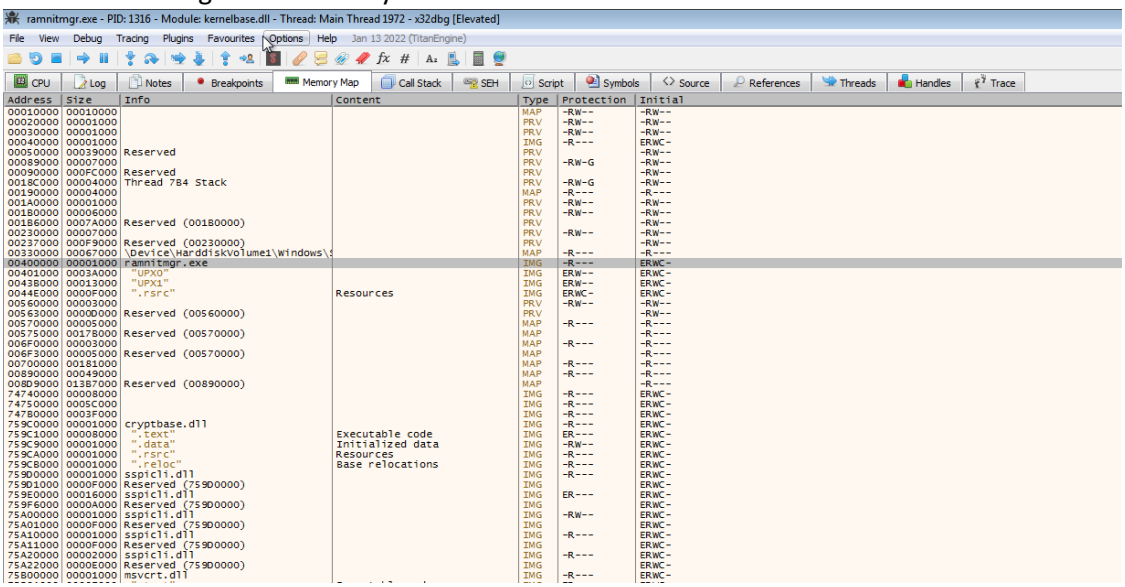
Now here we again hit the VirtualProtect and now view the second parameter in memory map and now it has again changed its permission to read only.



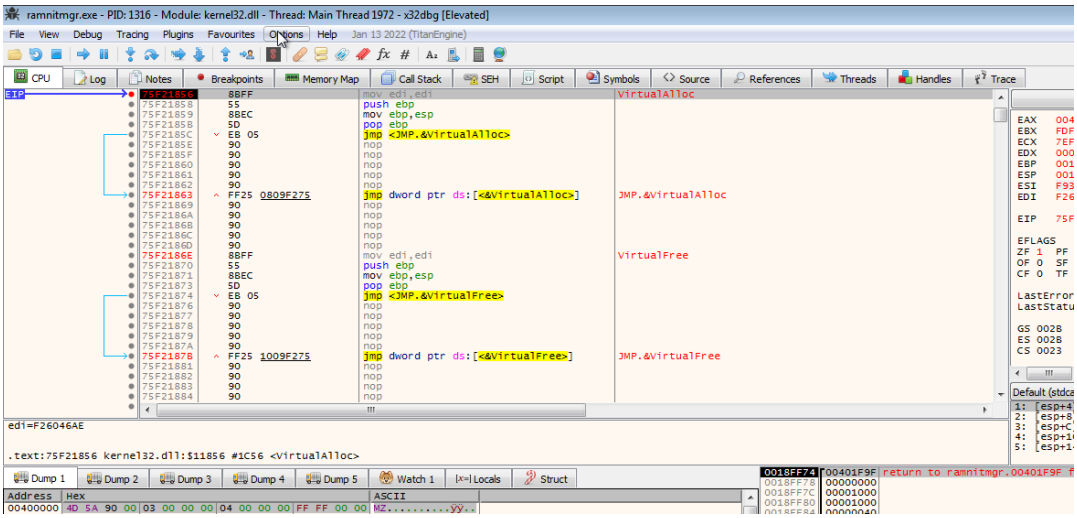
Just Before the call.



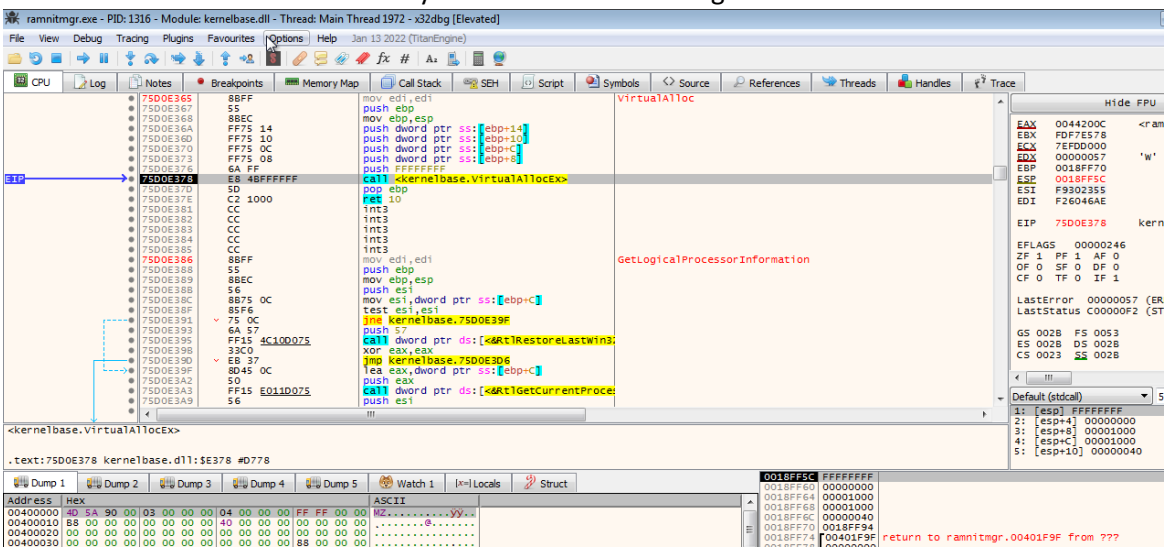
Permission changed to read only after the call.



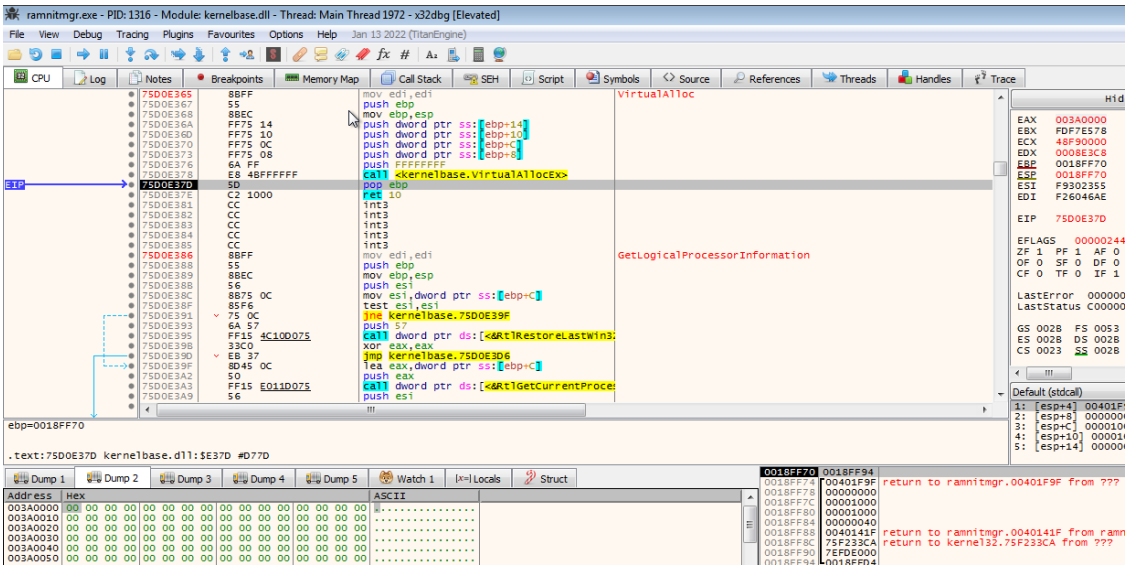
Now we hit breakpoint at VirtualAlloc



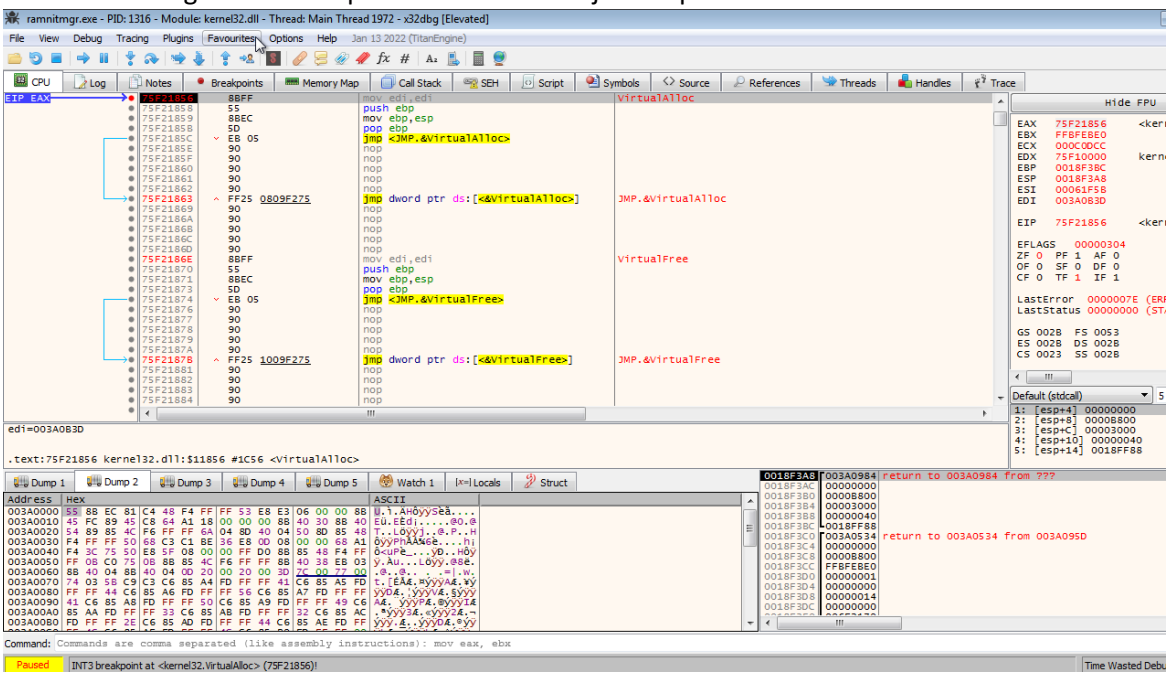
After this call the allocated memory will be shown in eax register.



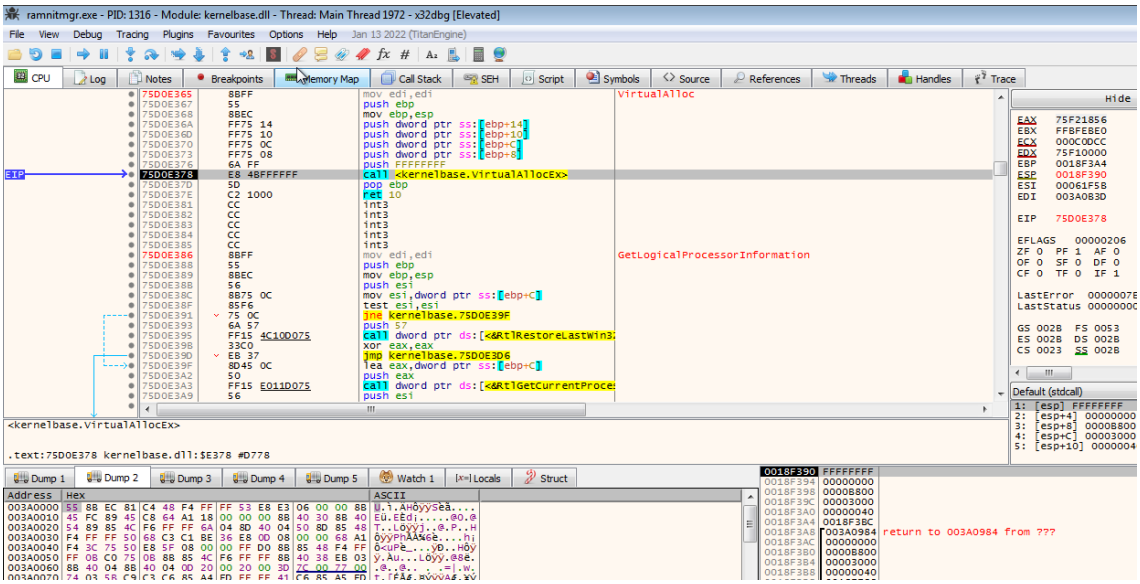
Here we can see the allocated memory is at 3A0000 and dump this location at dump1.



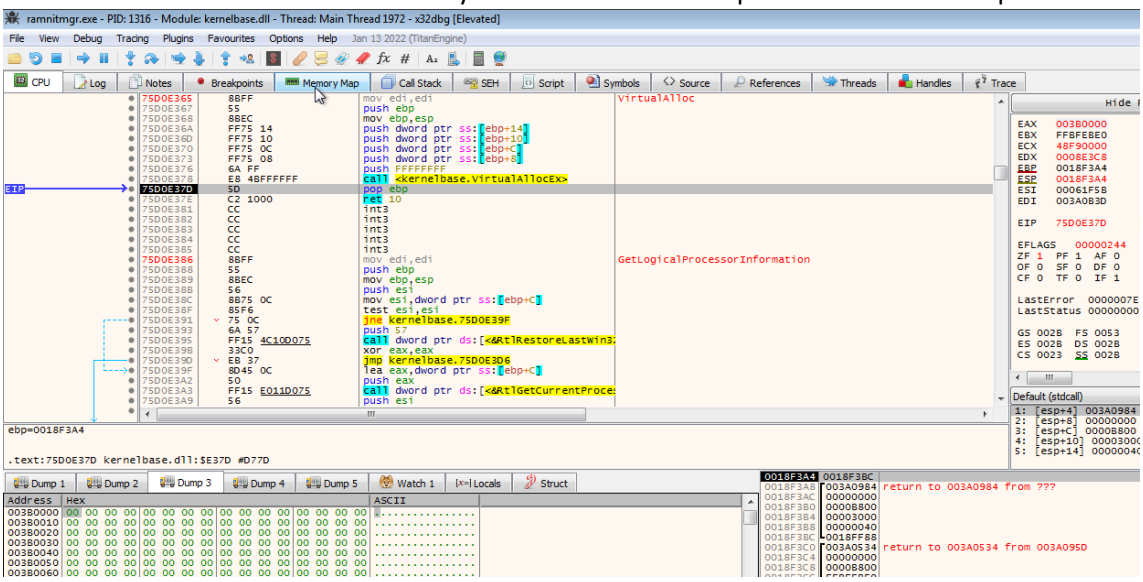
Now here we again hit breakpoint at VirtualAlloc just step over it.



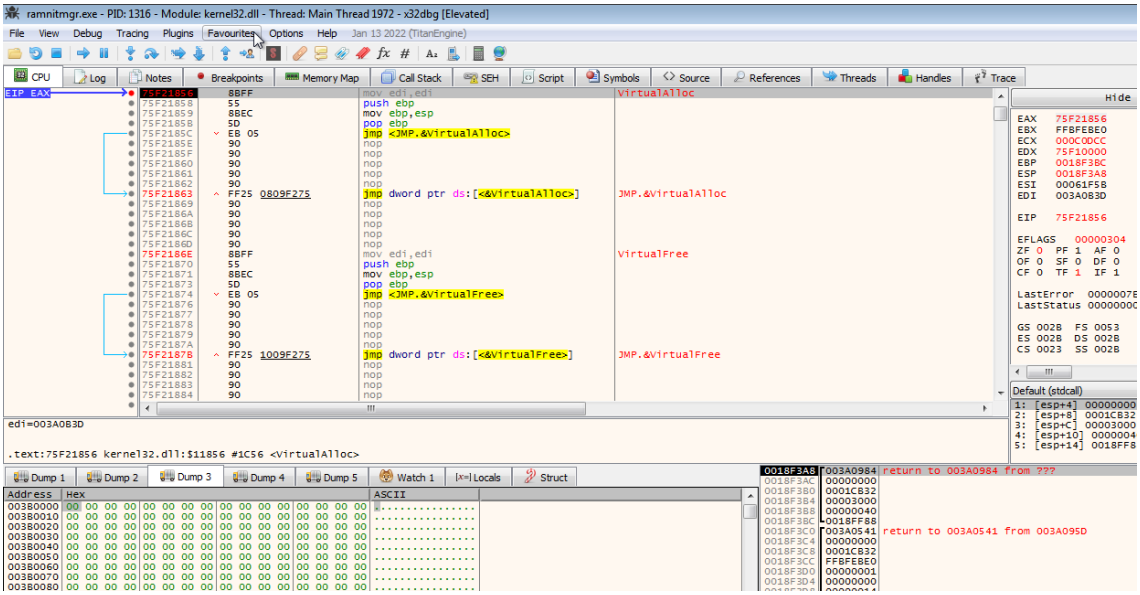
Now After this call the allocated memory will be shown in eax register .



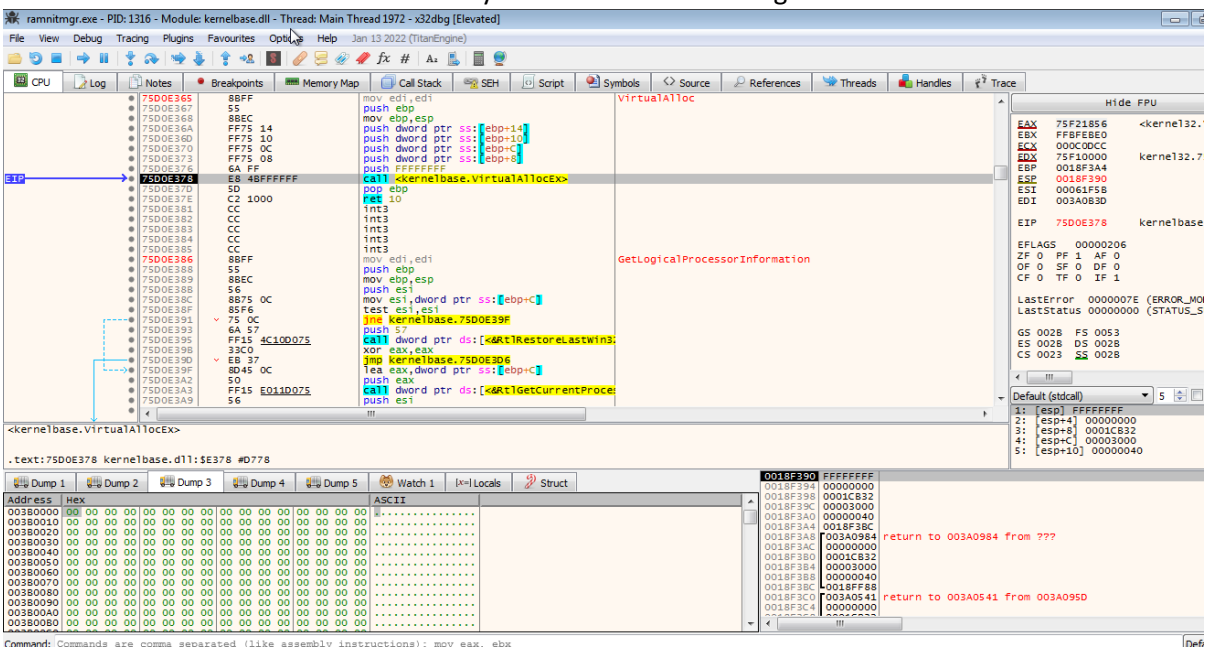
Here we can see the allocated memory is at 3B0000 and dump this location at dump3



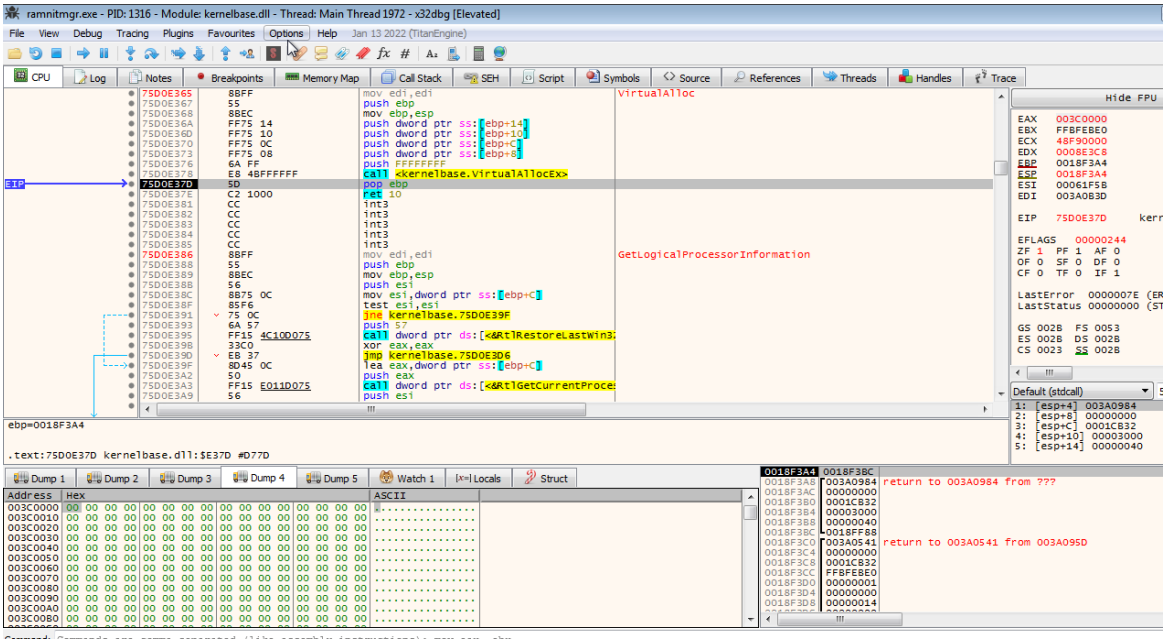
Now here we again hit the VirtualAlloc just step over it .



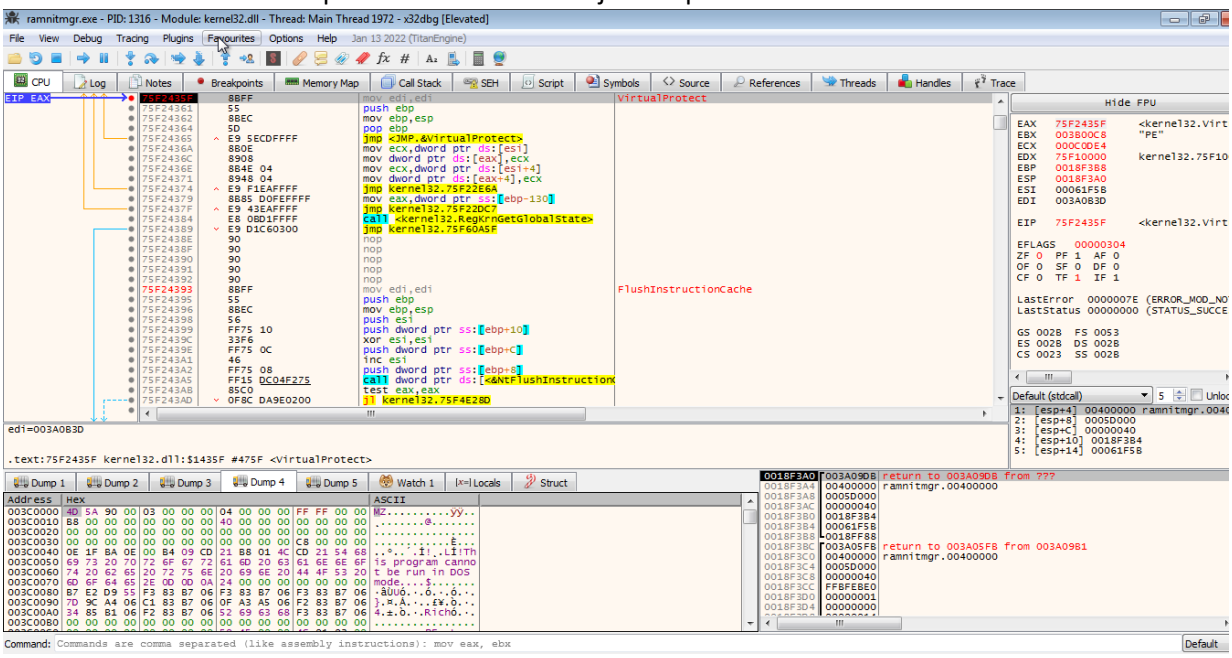
Now After this call the allocated memory will be shown in eax register



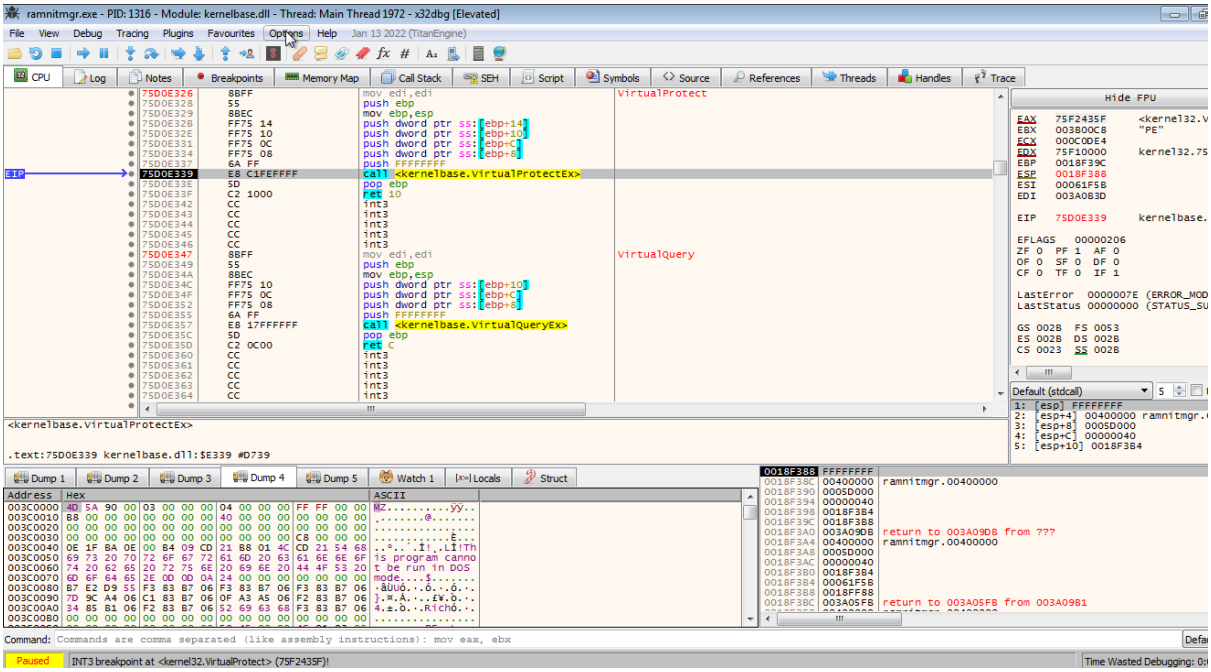
Here we can see the allocated memory is at 3C0000 and dump this location at dump4



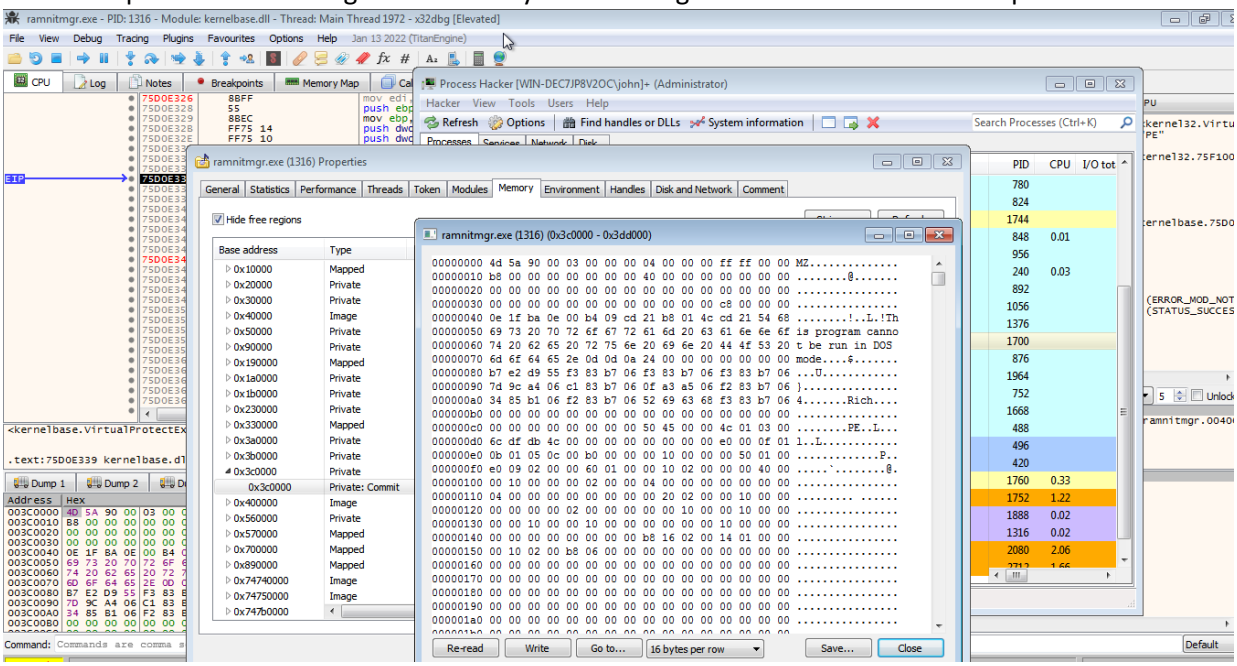
Now here we hit the breakpoint at VirtualProtect just step over it.



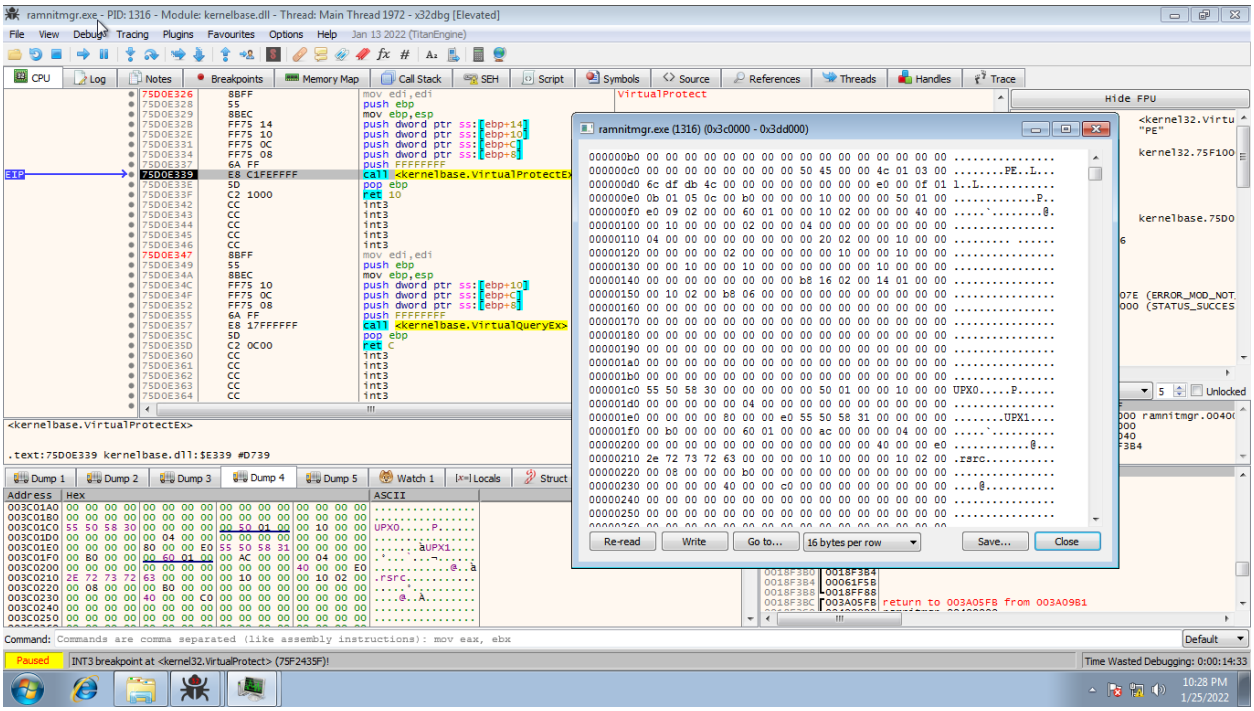
Now here note the second parameter address that is the region whose permission bits will be changed.Now as unpacking has been completed now we will dump it using process hacker.



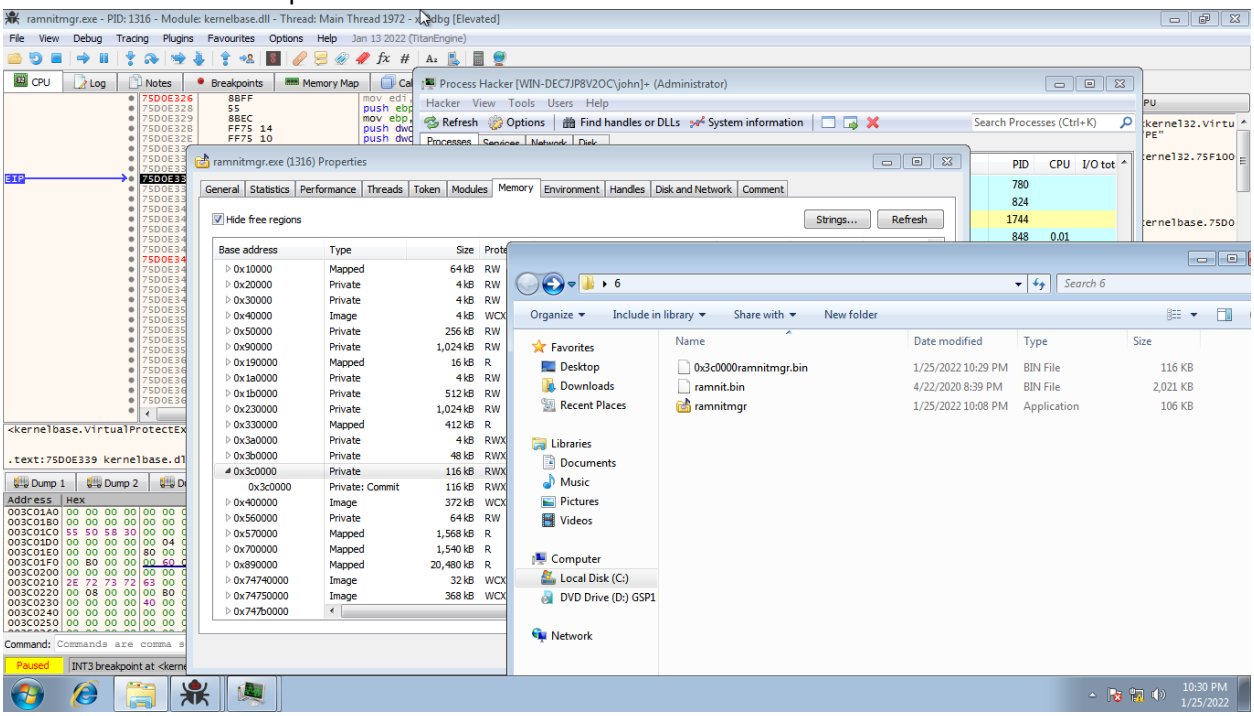
Here we open the 3c0000 region of memory at ramnitmgr.exe and now we will dump it.



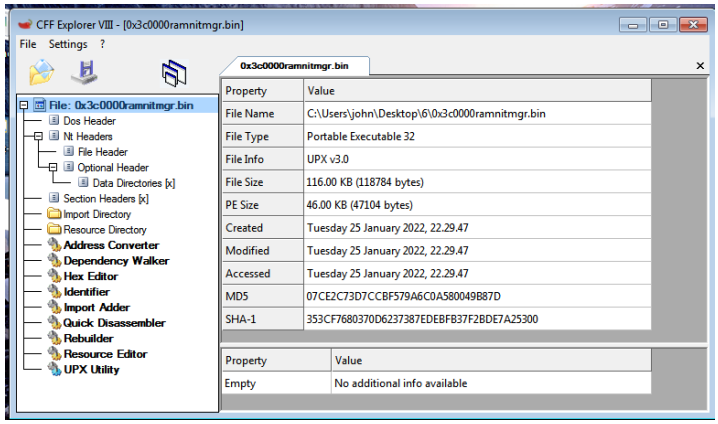
Here we can see that it might be packed with packer like upx so here we can use CFFExplorer to further unpack it.



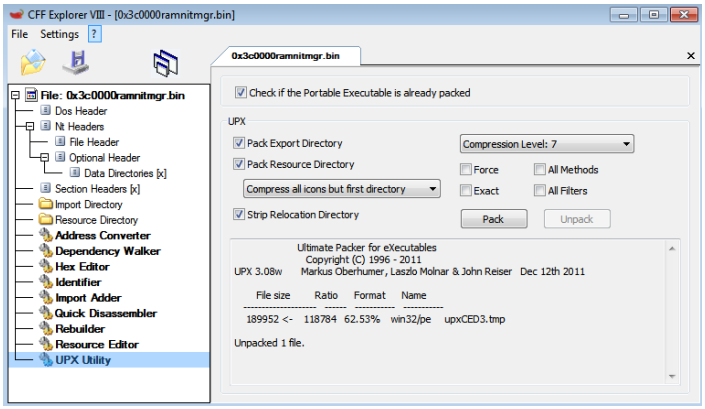
Now here we have dumped the file.



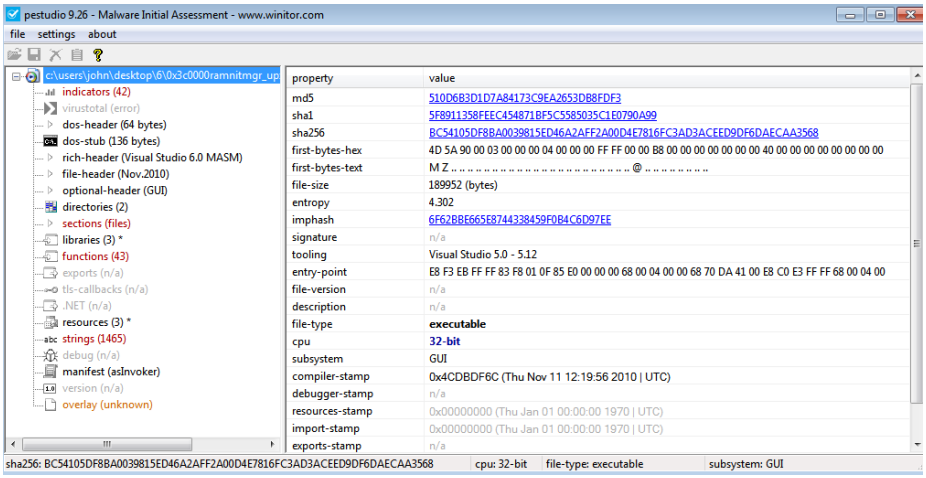
Now here we are using CFF Explorer to unpack it and here it has recognised that it is packed with UPX v3.0.



Now click on UPX Utility tab and click on unpack button and here it had successfully unpacked it now save it.



Now we can load the unpacked sample in pestudio and analyse it.



Here we can note the suspicious APIs that it is using.