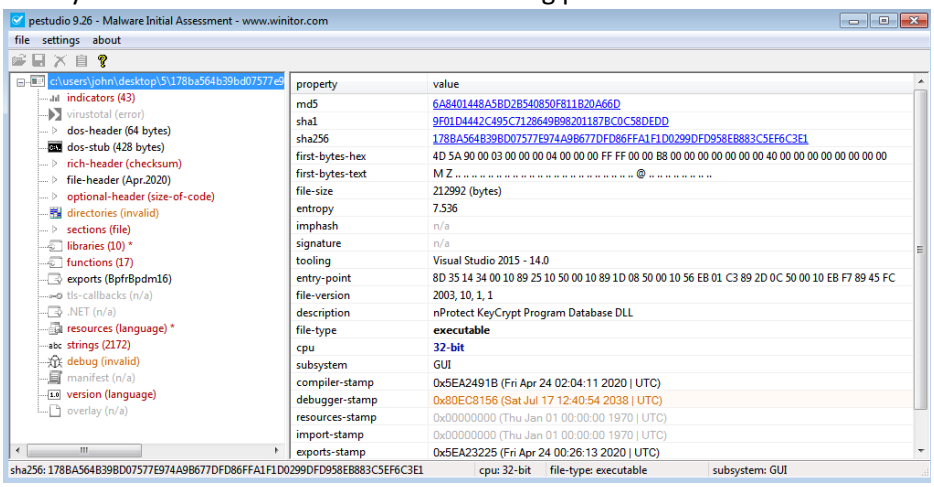
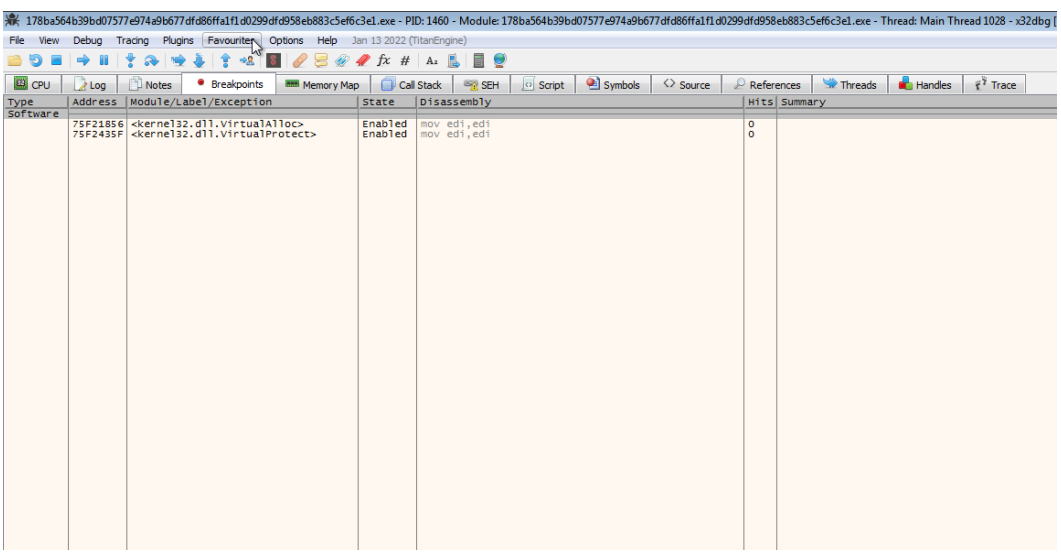
Intially we calculated the hash of the file using pestudio.



The highest entropy value can be 8, but here it is 7.538 which is close to 8 so we can assume that it is packed.

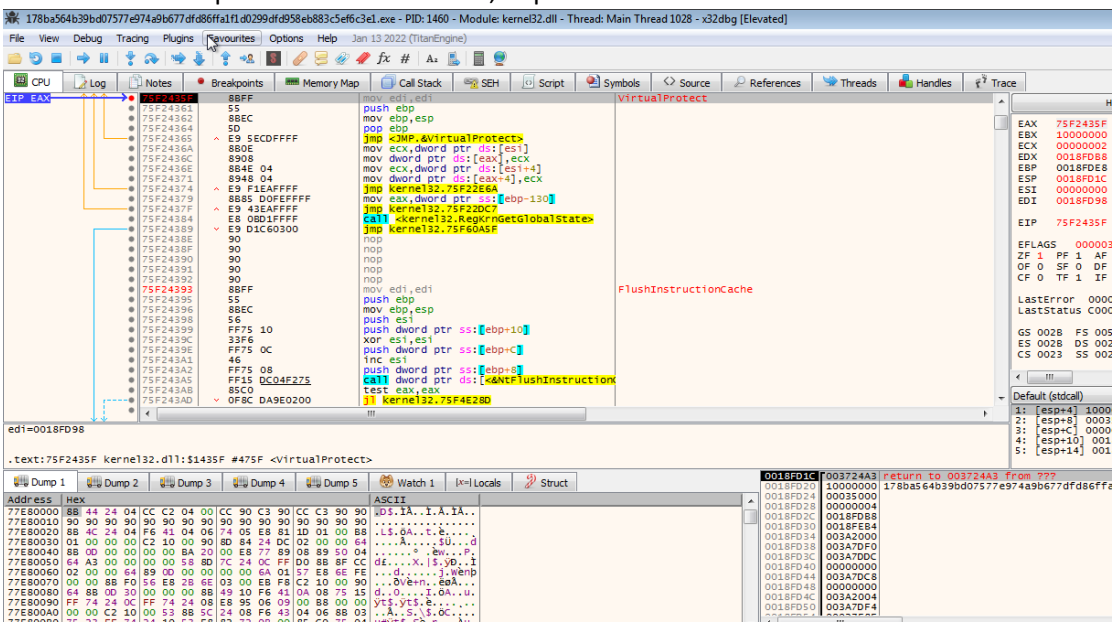
The other method to note that a file can be packed by either using detect it easy or by loading in IDA in IDA it will show us warning like Corrupted Fixup Table or it will have less imports or function name.

Now we load the program in x32dbg. Here after loading we will put two breakpoints VirtualAlloc and VirtualProtect.

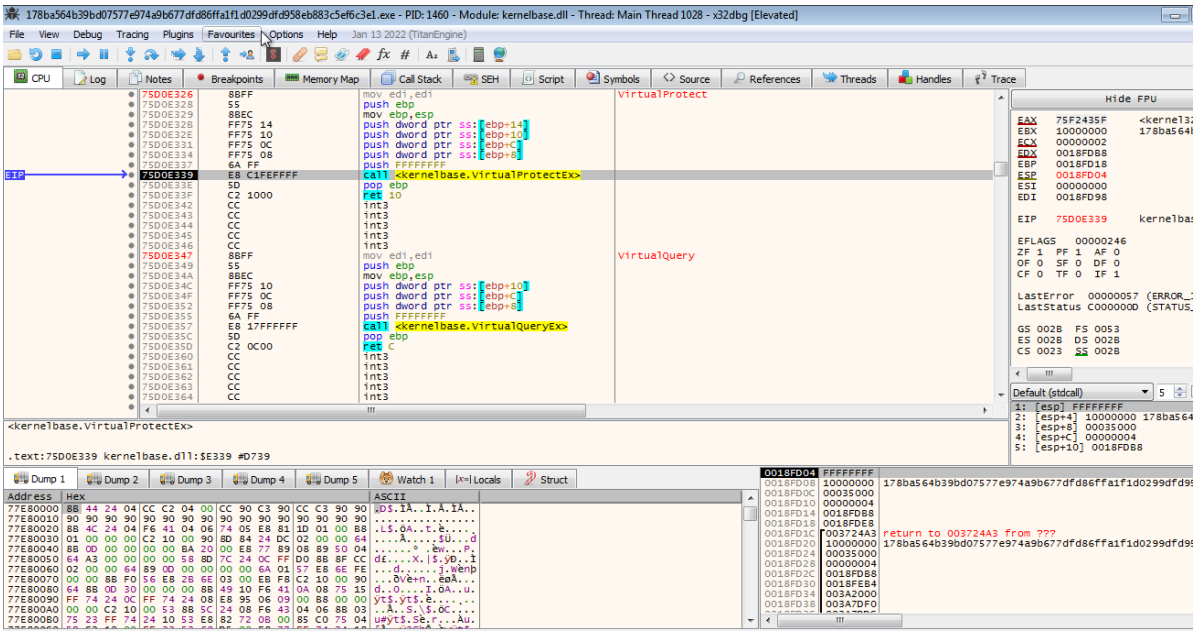


Initially run the sample we got breakpoints at VirtualAlloc, one can check out the memory allocated by VirtualAlloc by pressing the upward arrow (i.e. execute till return) and then on eax we can right click and dump the memory returned by VirtualAlloc, but here we didn't find anything useful using VirtualAlloc, after 3 calls of VirtualAlloc, we got VirtualProtect.

Now we hit breakpoint at VirtualProtect ,step over it.

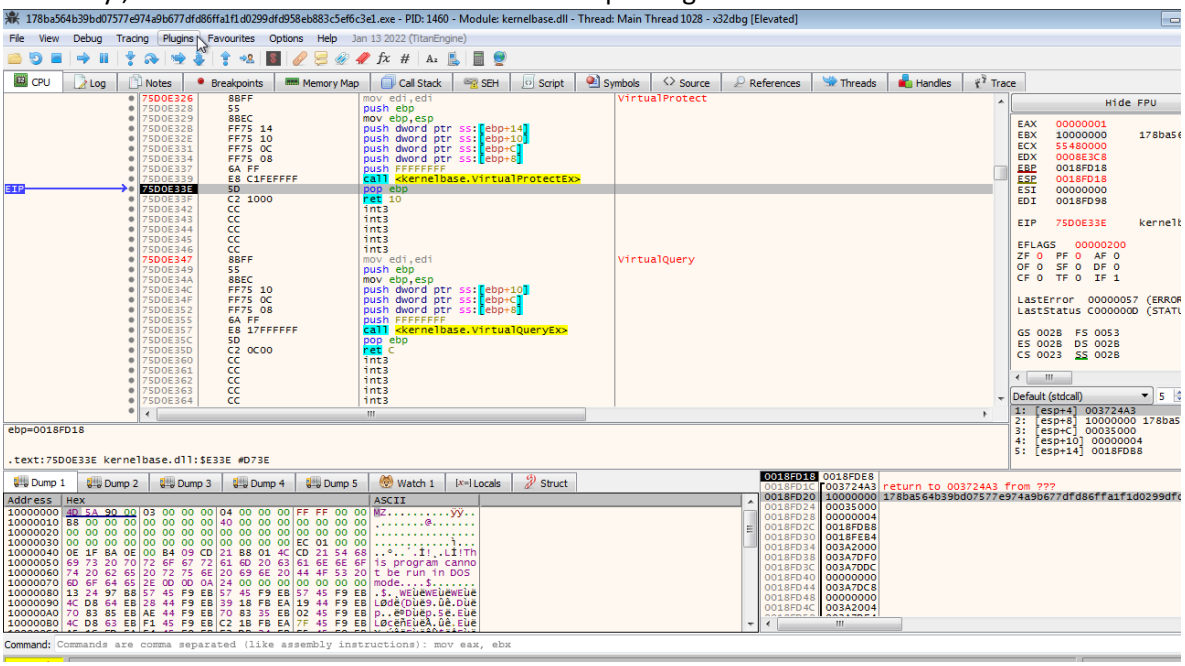


Now in this below image we can see the second parameter (i.e. 10000000) this is the location the VirtualProtect has changed the permission.

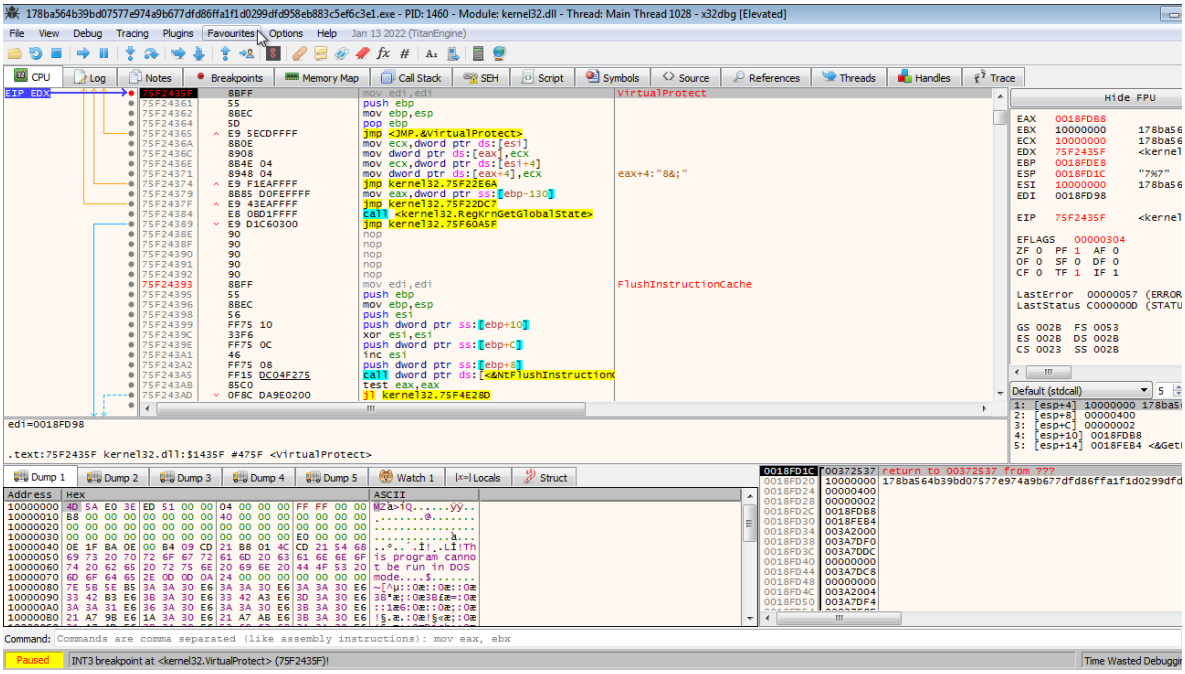


Now here we again hit the VirtualProtect, now here dump the second parameter i.e. 10000000 in dump1 ,if we view this address in memory map previously it was read,write and after call it become

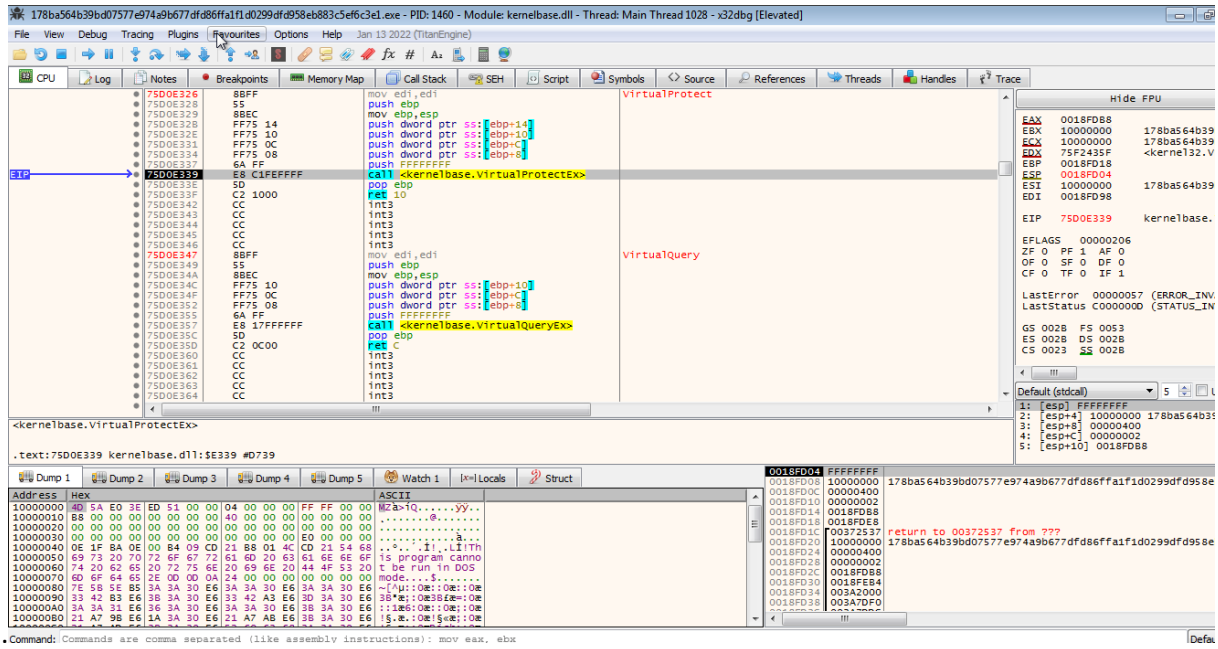
read only , we can conclude that it had finished unpacking at 10000000.



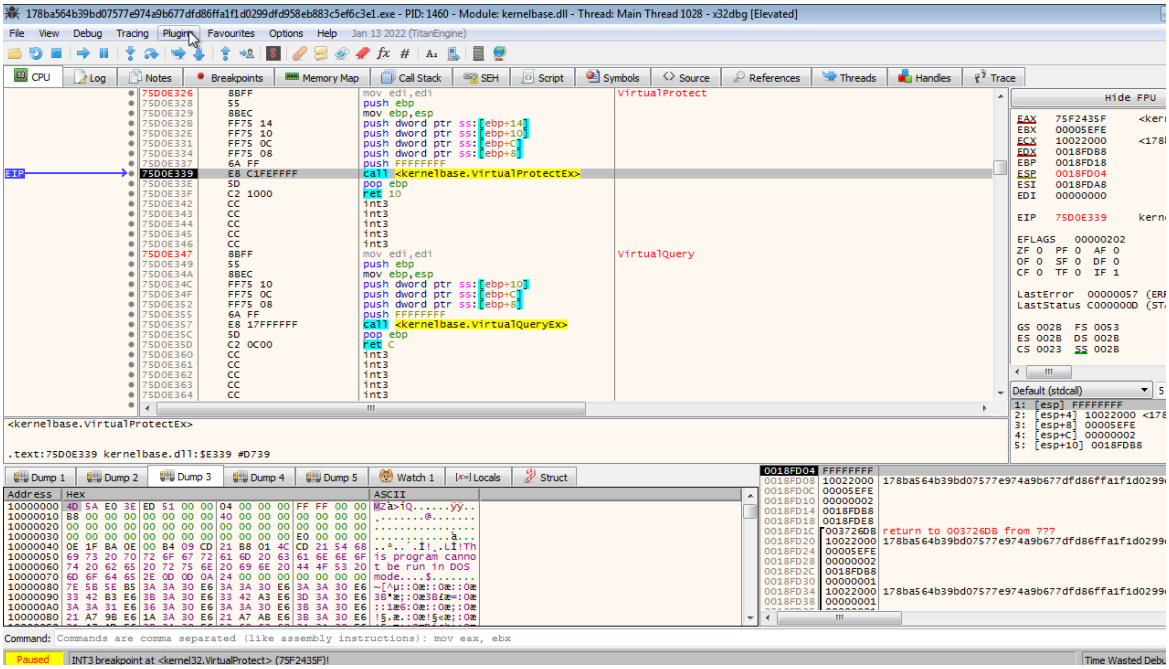
Now we again hit the VirtualProtect , just step over.



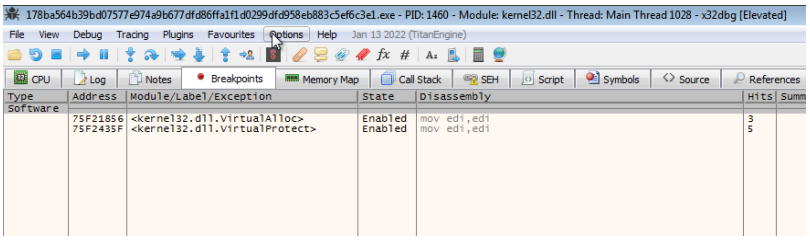
Here just step over, and note the second parameter .



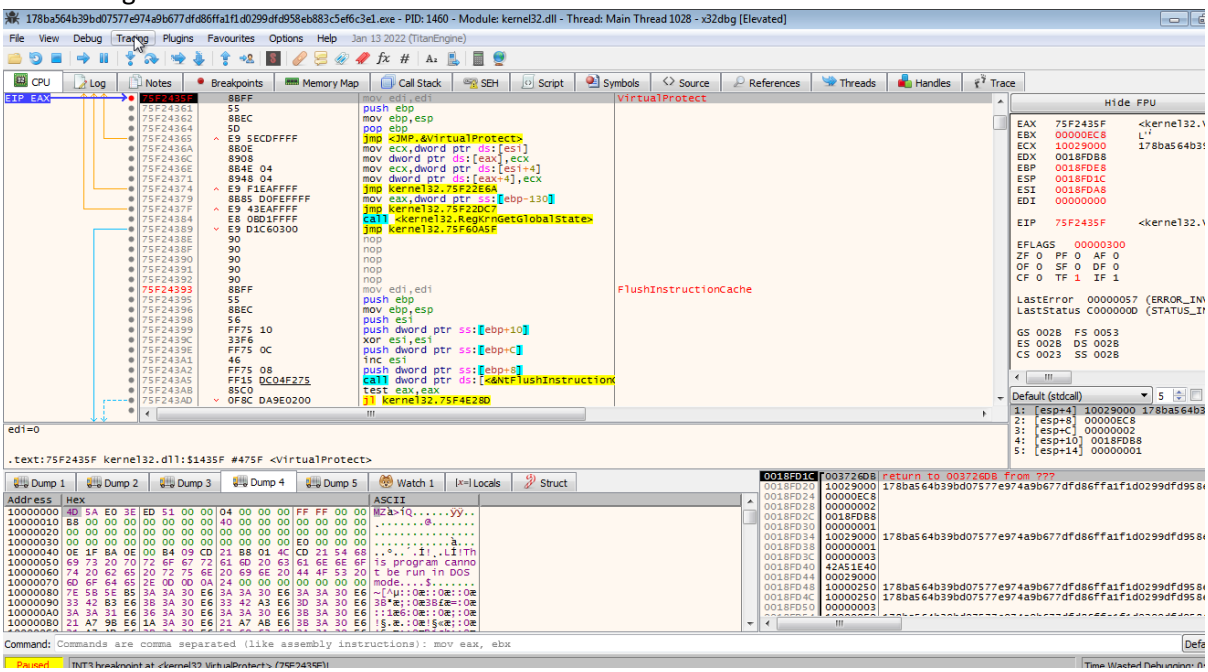
Now we again hit the breakpoint at VirtualProtect and note the second parameter mention is continuation to the previsouly change bit region 10022000.



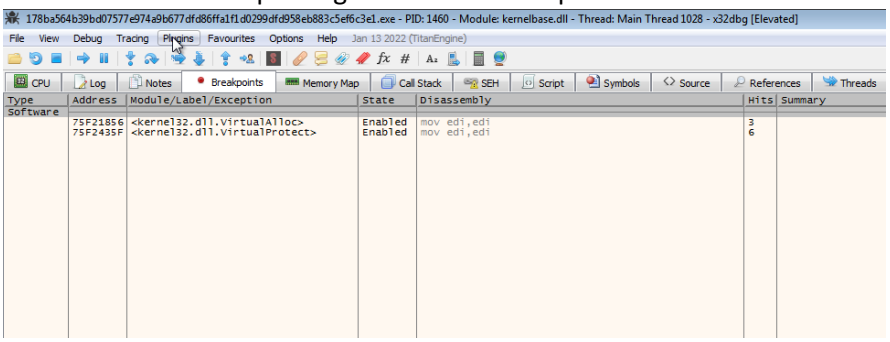
Till now we have hit the VirtualAlloc 3 times and VirtualProtect 5 times.



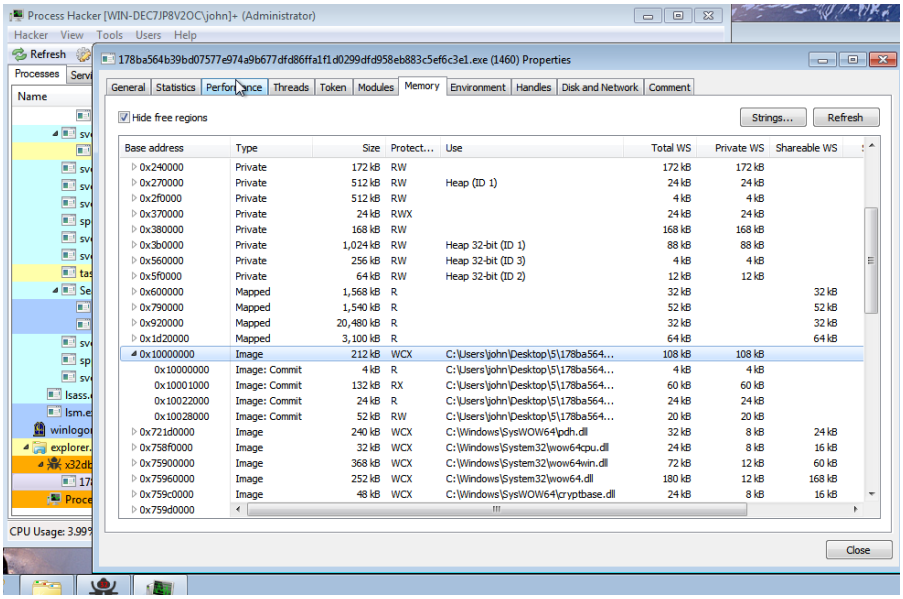
Now we again hit the VirtualProtect.



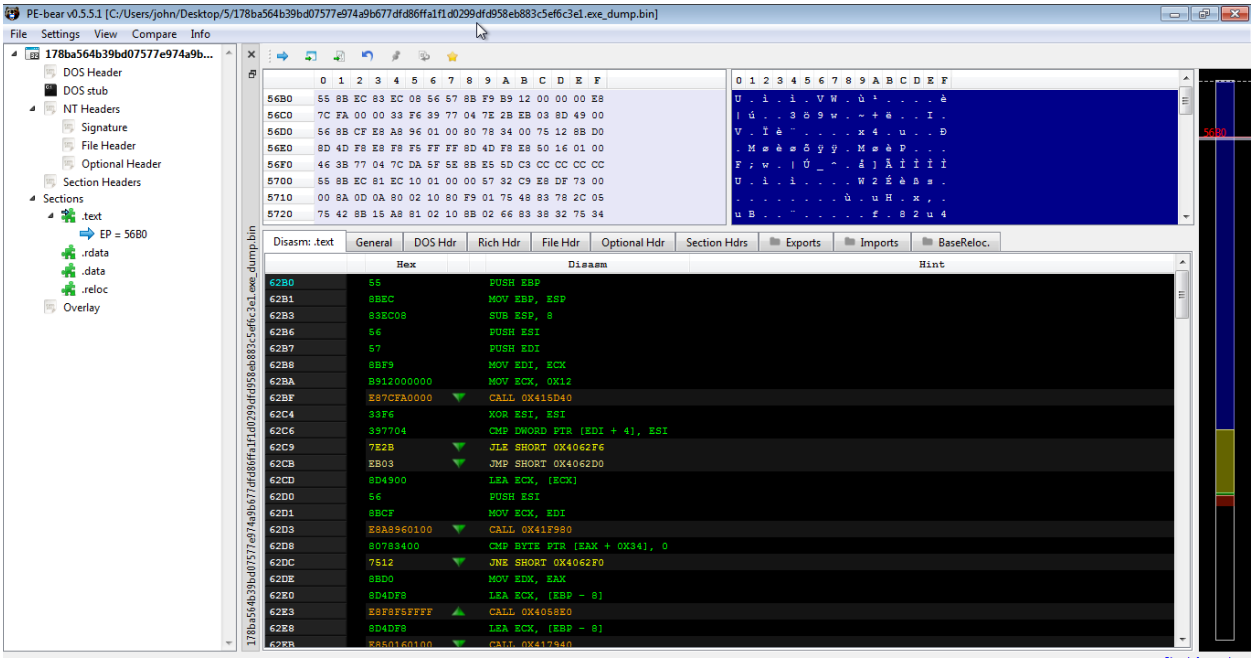
Now here as we know we will get an exception after VirtualProtect has been called 6 times, that means it had finished the unpacking now we can dump it .



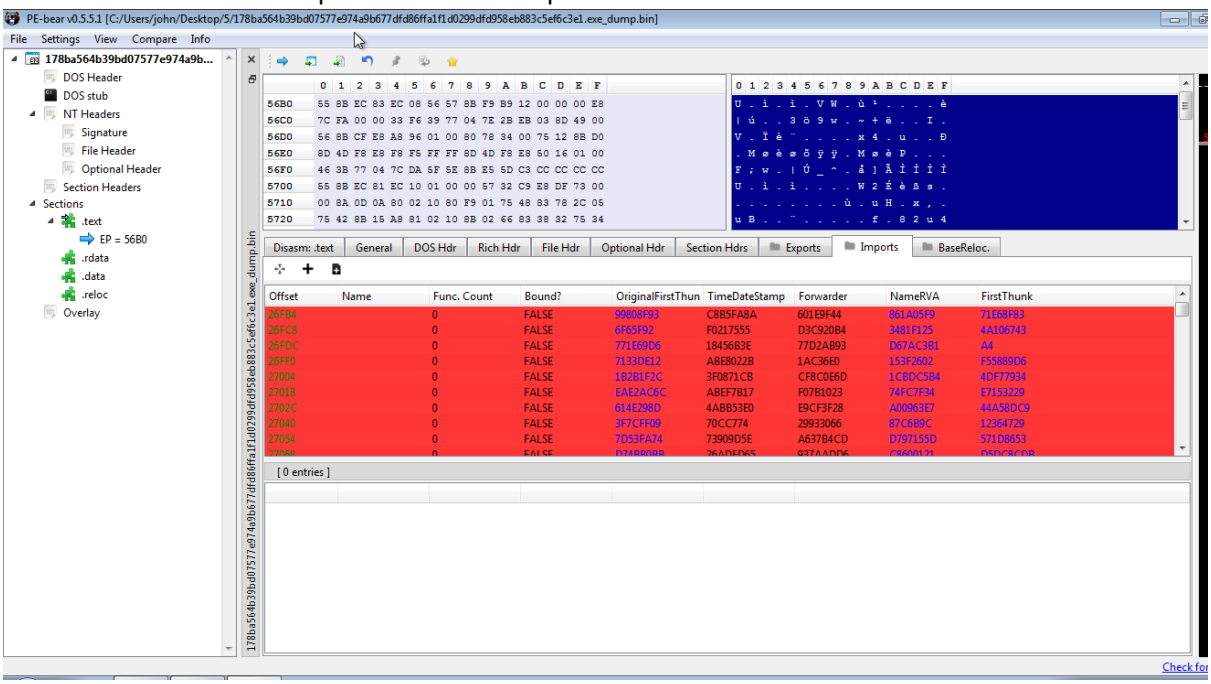
This malware is self injecting, so that means it will overwrite it process , so Now we can dump this using process hacker , double click on dridex and open memory tab and dump it by right clicking on memory location at 10000000.



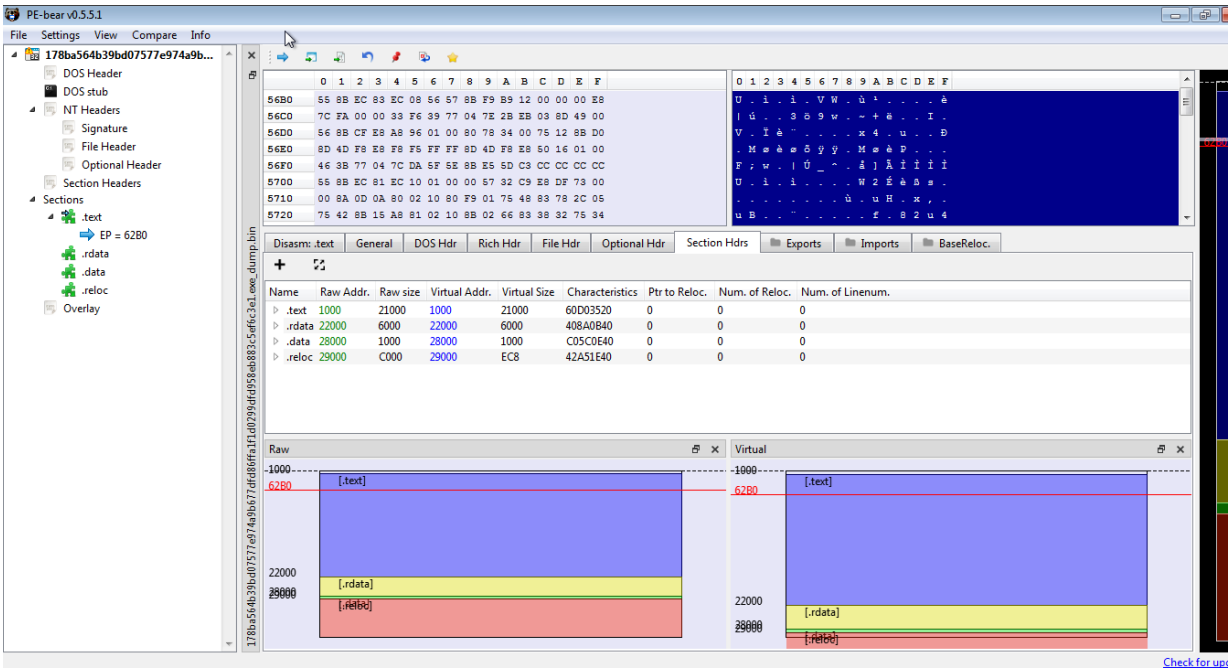
Now we will unmap the dumped file using PE-bear.



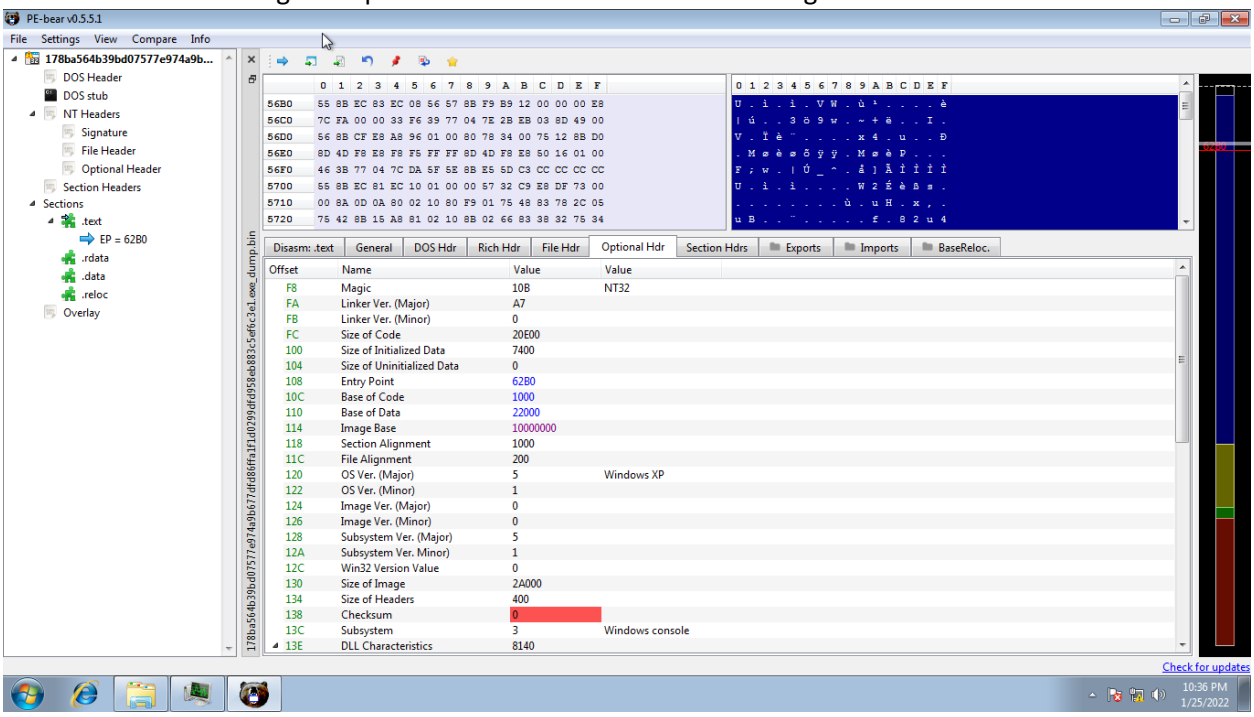
Here we can see all the imports are messed up.



So now here we will fix the section header , intially we will make raw addr. Same as virtual addr. And then calculate the raw size and then make the virtual size same as raw size.



Now after that we will go to Optional Hdr. Tab and then fix the image base to 10000000.



Now here we can check the name in exe i.e. ldr.exe which is loader for dridex, now we can dump it.