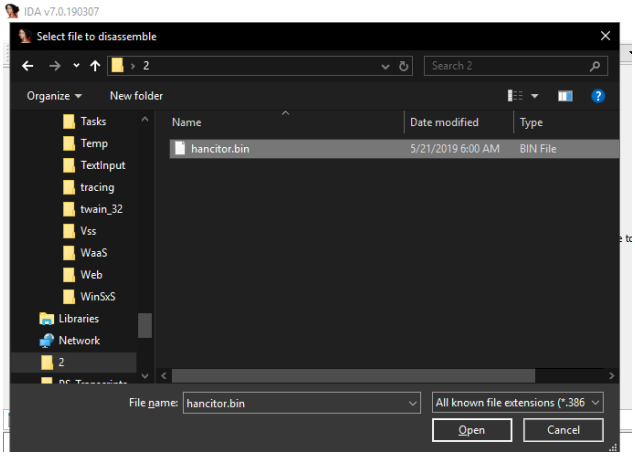
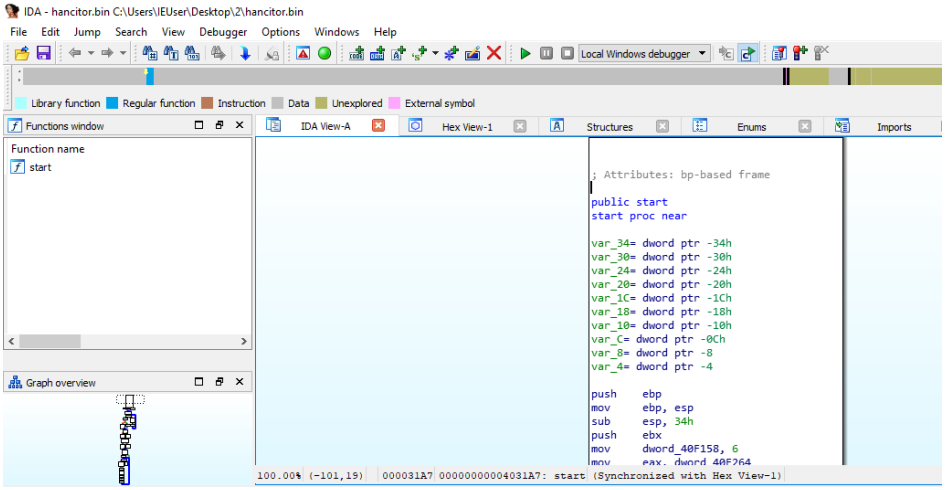
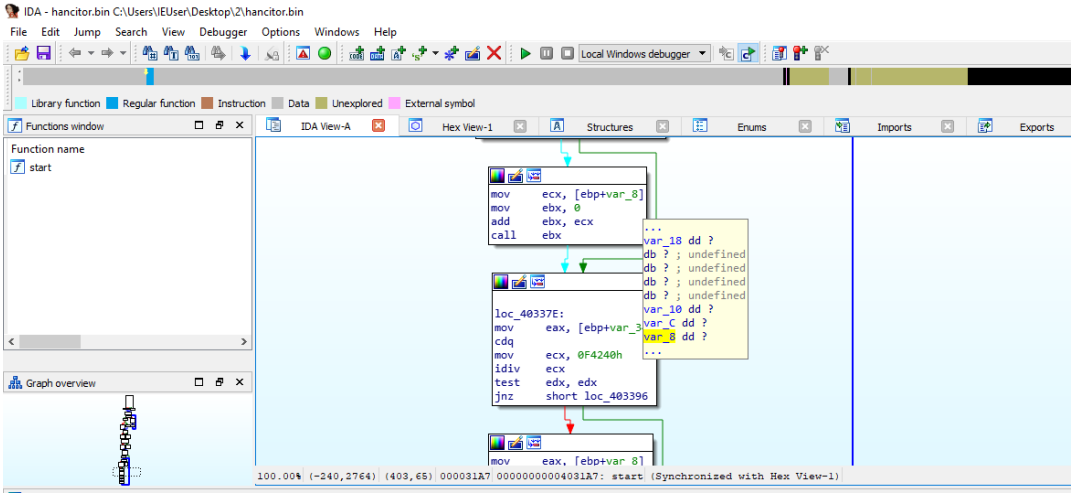
Initially we will load the sample in IDA to know whether it is packed or not .



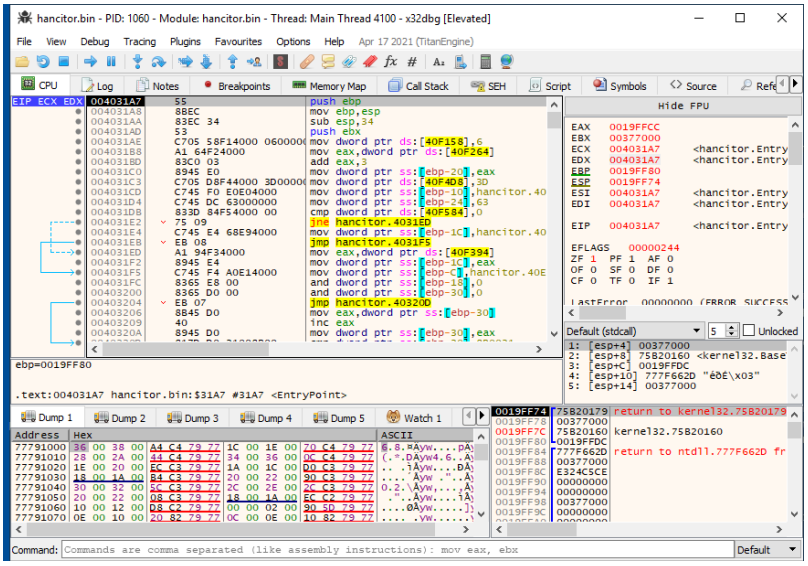
Here in IDA as we can see in fuction name window there is only one function , it means the sample is packed.



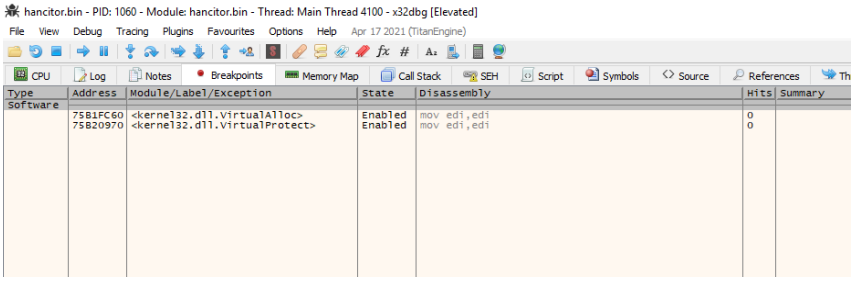
Call to register are highly suspicous either it can be calling routine to unpack the code or may be call the code that have been already unpacked.



Now we will load the sample in x32dbg.

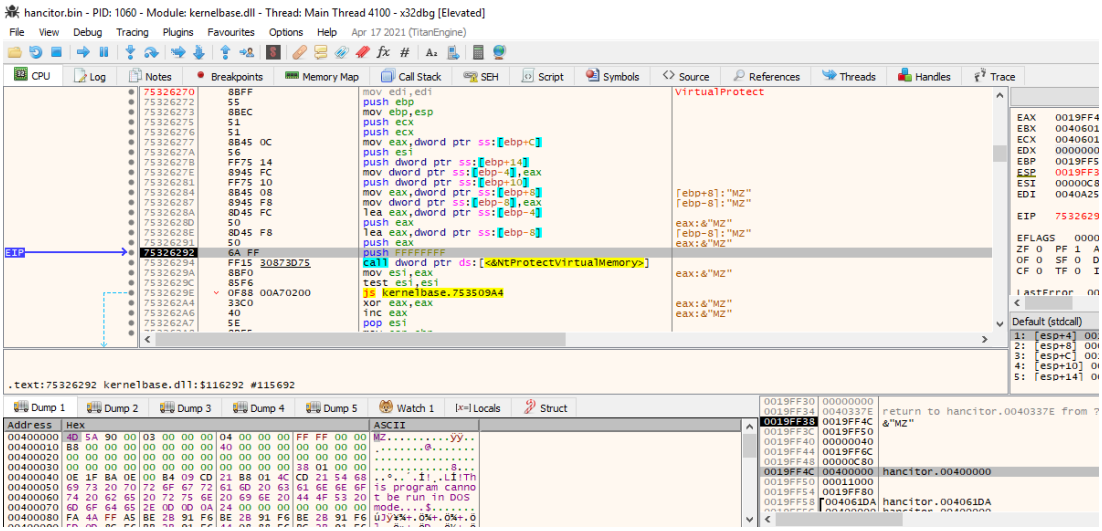


Now we will set breakpoint at VirtualAlloc(used to allocate memory for unpacking code) and VirtualProtect(used to change the permission bits for the memory).

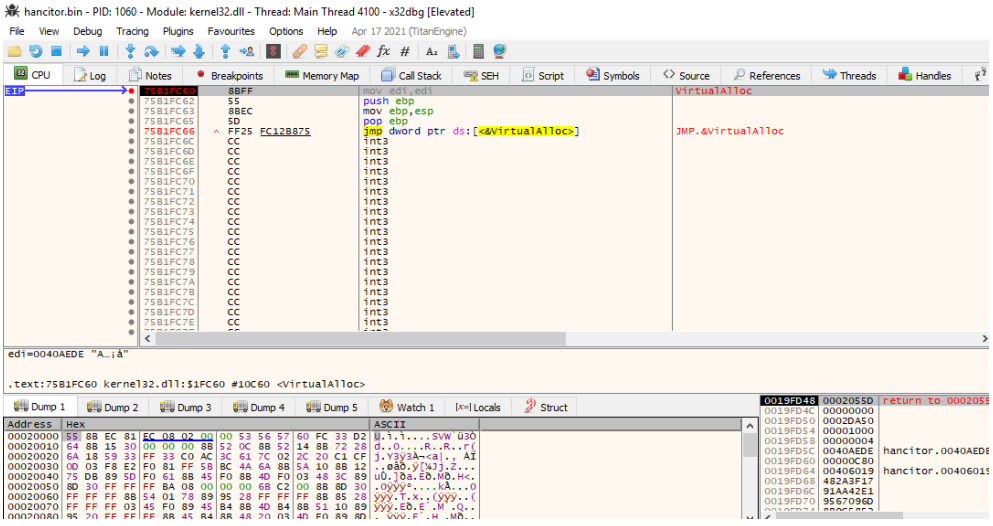


After here Note the number of time the VirtualAlloc(7) and VirtualProtect(1) have been hit.Now restart the machine from snapshot taken and again load the saampe in x32dbg and put breakpoint on VirtualAlloc and VirtualProtect.

Here we hit our first breakpoint just step over it, and load the second parameter of NtProtectVirtualMemory this is the region where the protection bits will be changed load that region in dump.

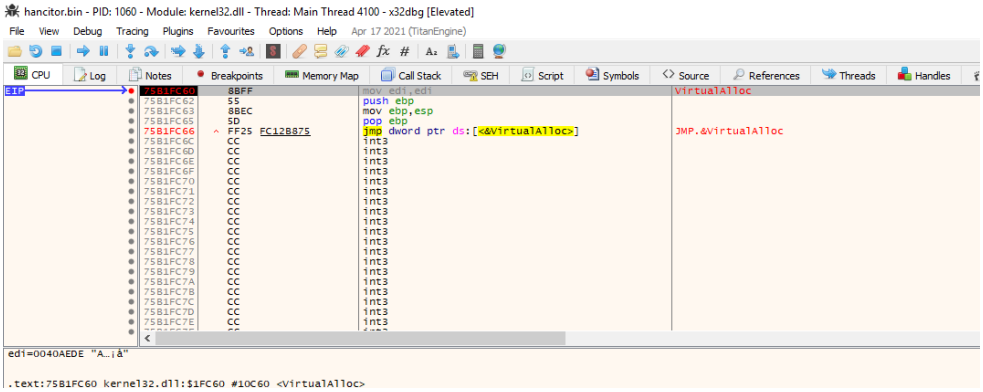


Now press run or f9. We will hit at VirtualAlloc step over (f8) it.

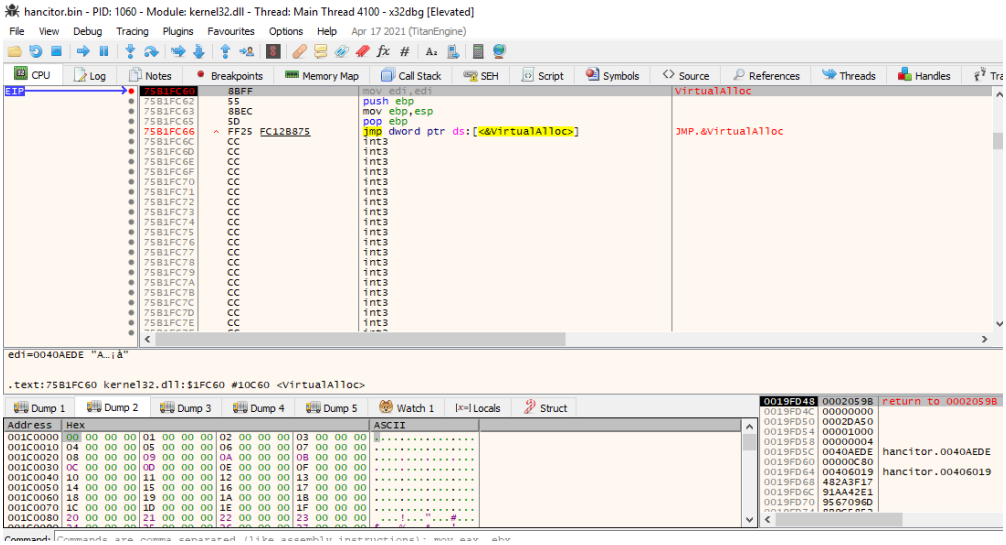


Now dump the value return by the VirtualAlloc i.e. in eax.

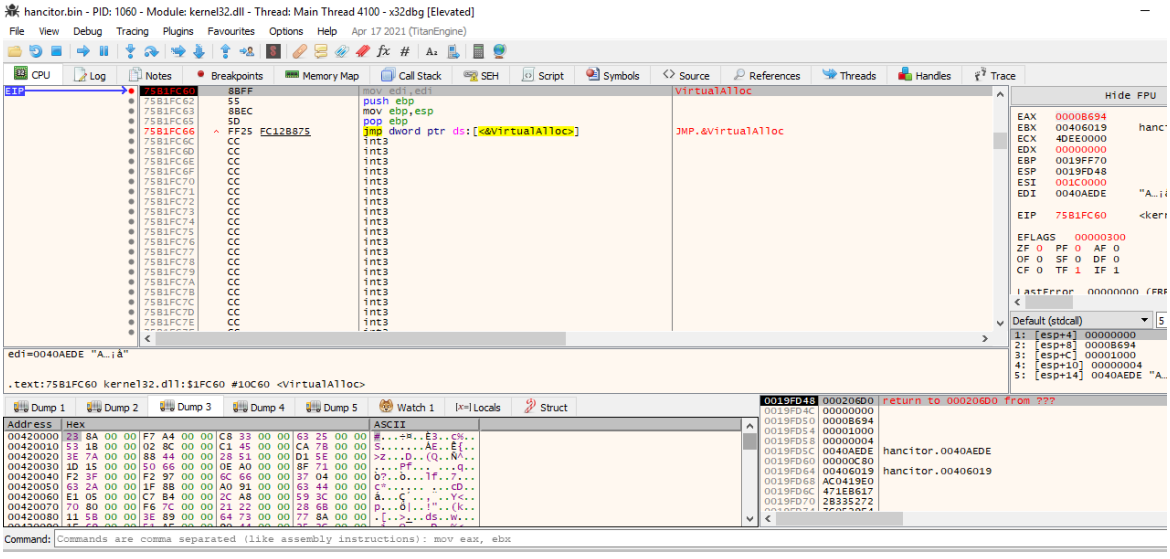
Here the previosuly dumped code contain the following GetModuleHandles, LoadLibrary APIs this is probably some intermediate code used to unpack exe file.Now we hit second VirtualAlloc and will review the return memory region by it i.e. eax.



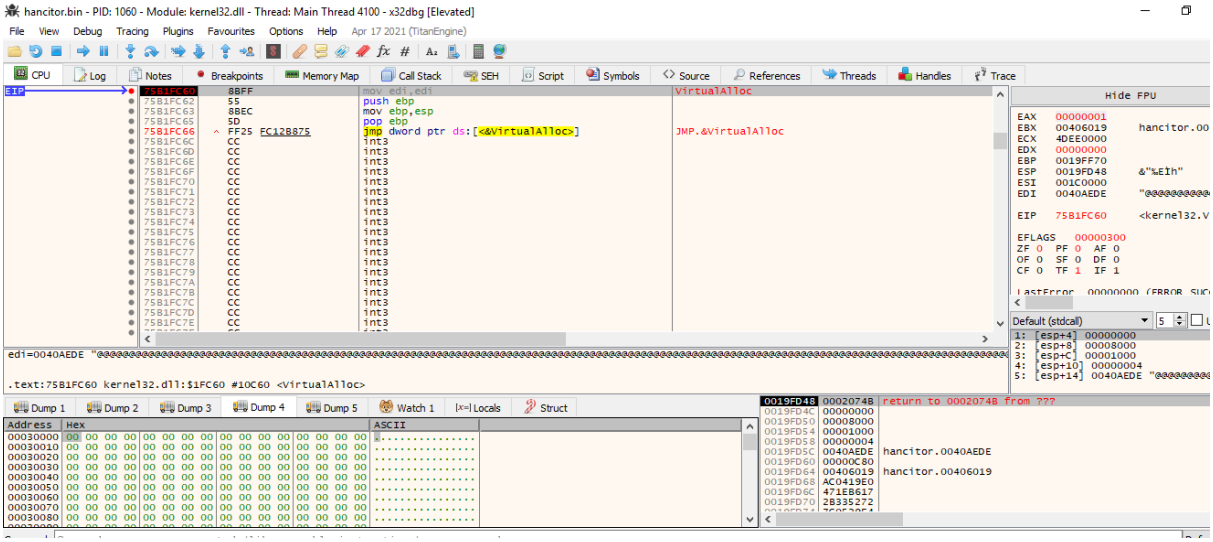
Press f9 and we will hit VirtualAlloc third time review the return memory region in dump.



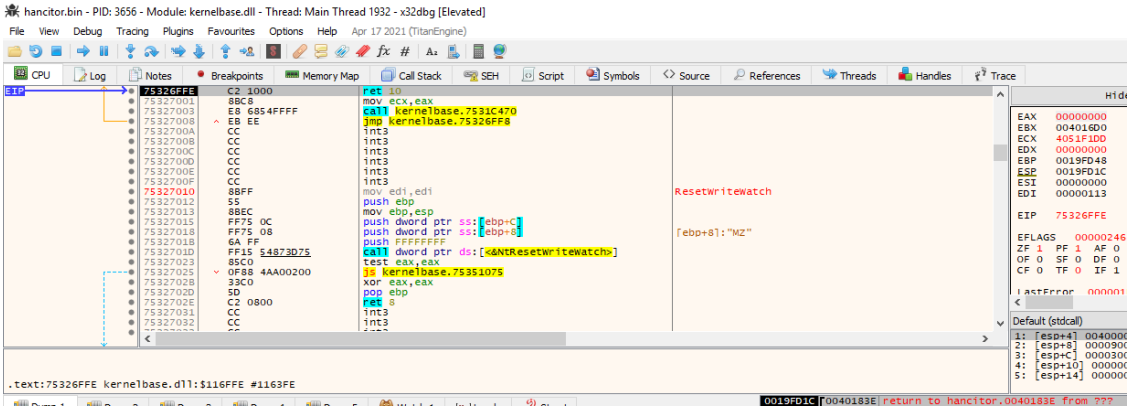
Press f9 and we will hit VirtualAlloc fourth time review the return memory region in dump.



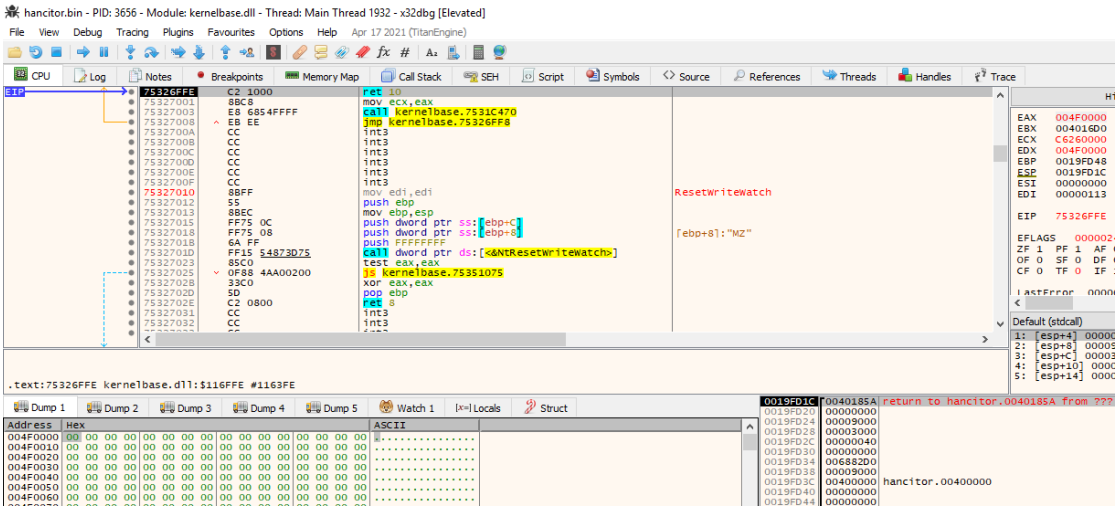
Press f9 and we will hit VirtualAlloc fifth time review the return memory region in dump now this time nothing will be present in dump. The sixth time VirtualAlloc will return the same memory location that we have already dumped in fifth call.



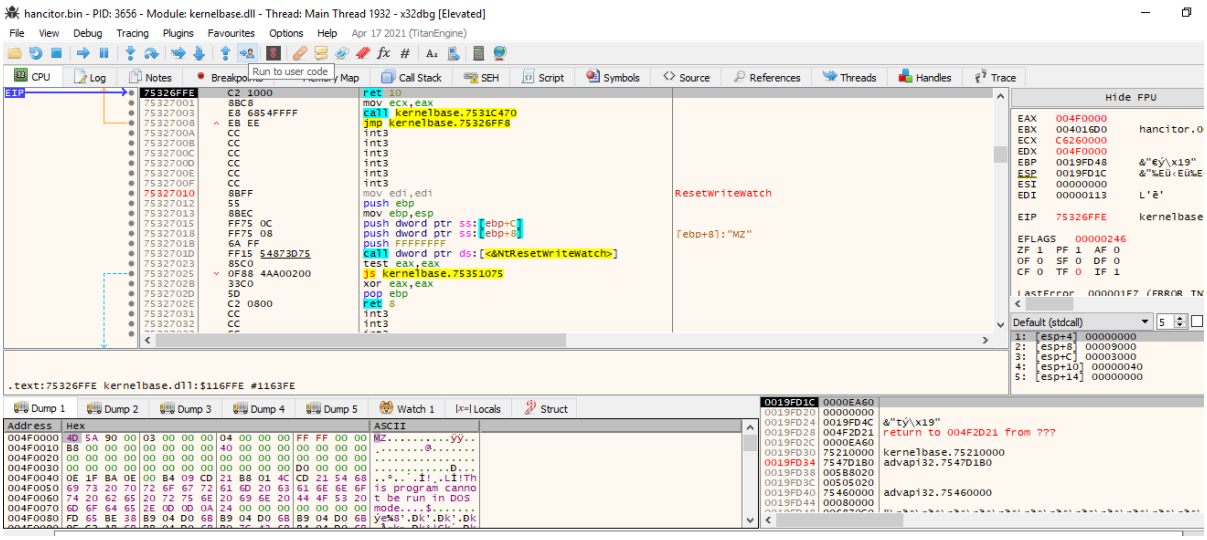
The sixth Virtual Alloc return the memory region 00000000 , we can't dump that so press f9.



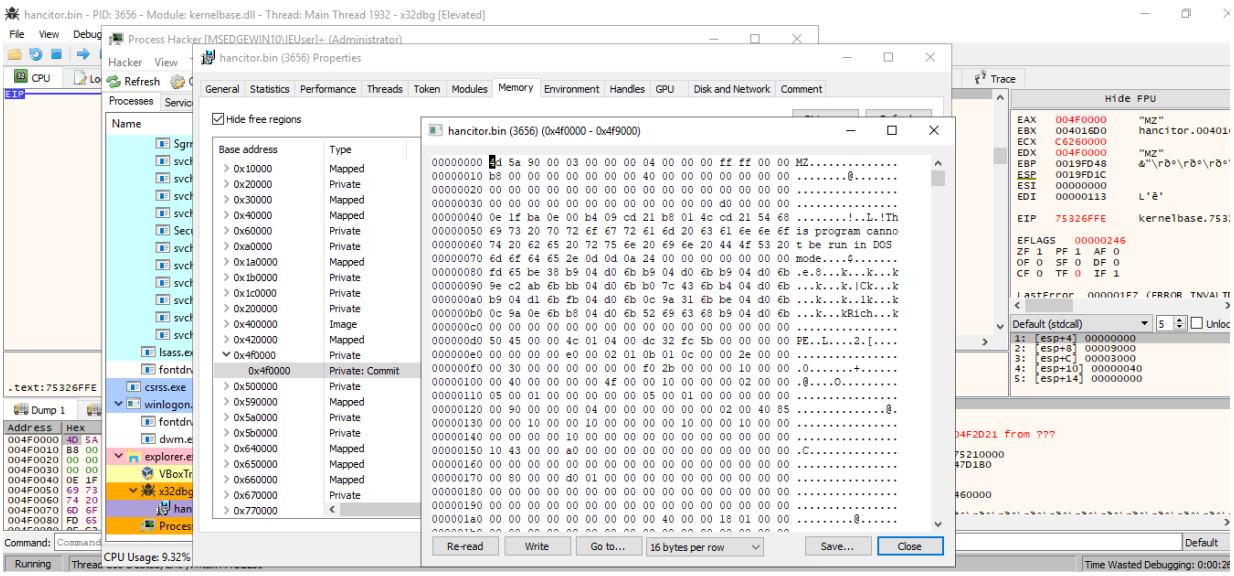
The seventh time VirtualAlloc returned the memory regoin 4F0000 so we will dump that region in dump1 and press f9.



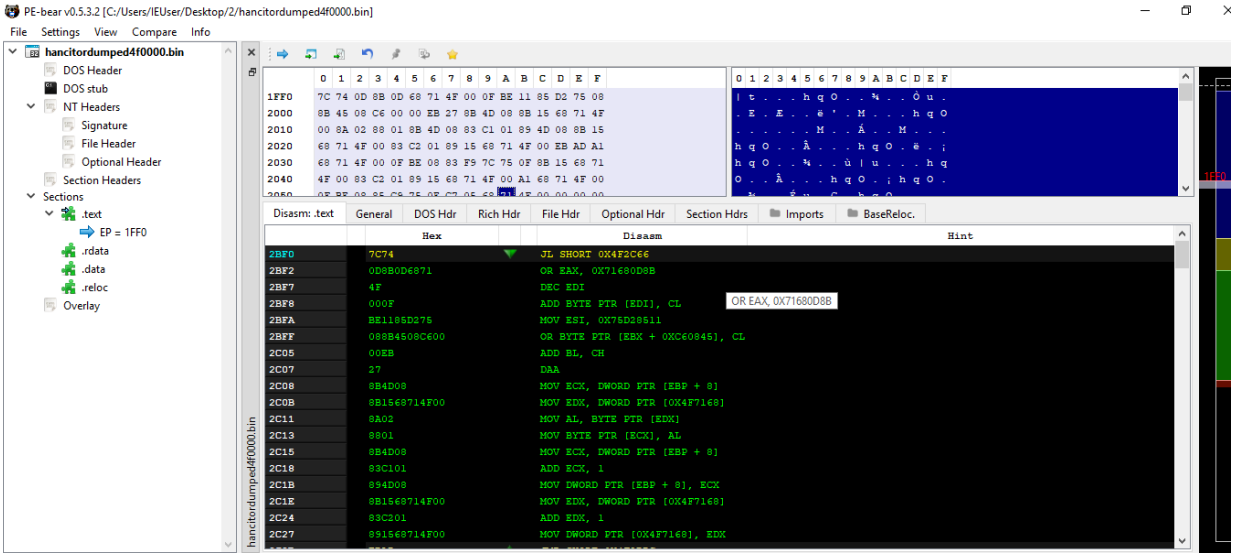
It looks like it have unpacked an executable



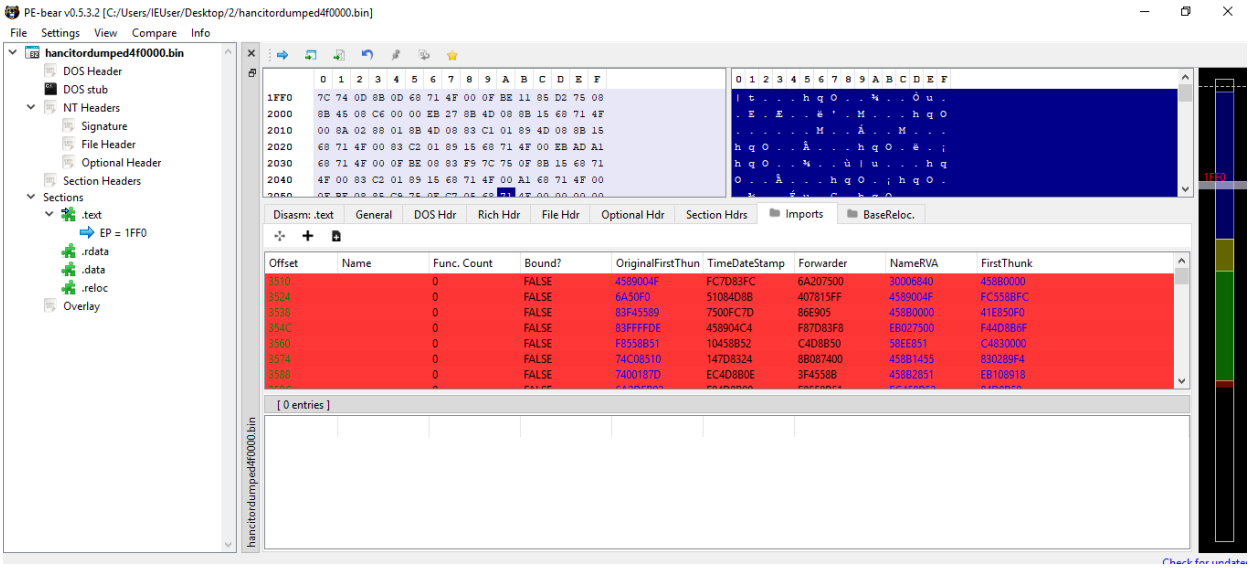
Now we will dump that exe using process hacker look for hancitor, double click it open memory tab in it and look for address 4f0000 so here permission bit is rwx double click on it we can view the executable and now right click on that address and save that exe.



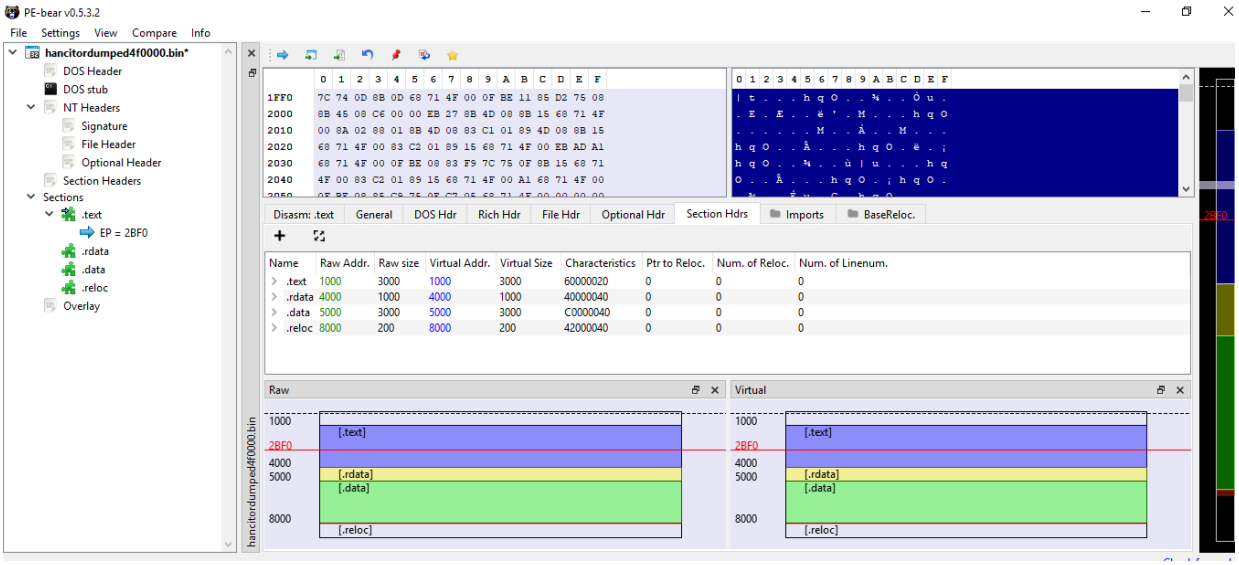
Now we will unmap it using pebear.



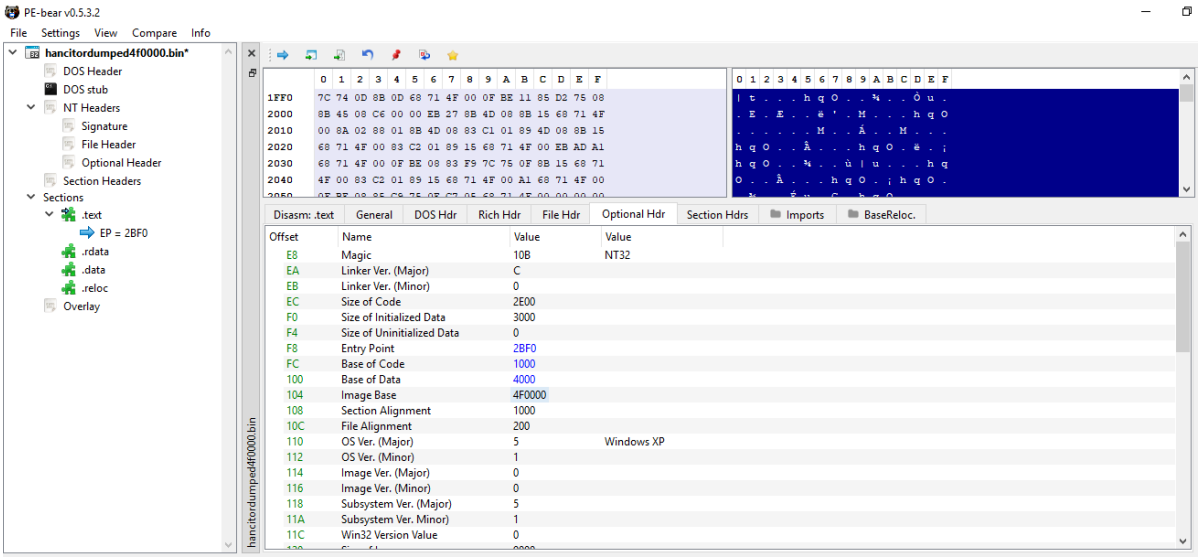
Open Imports tab it is all jumbled up, we will fix it using section headers.



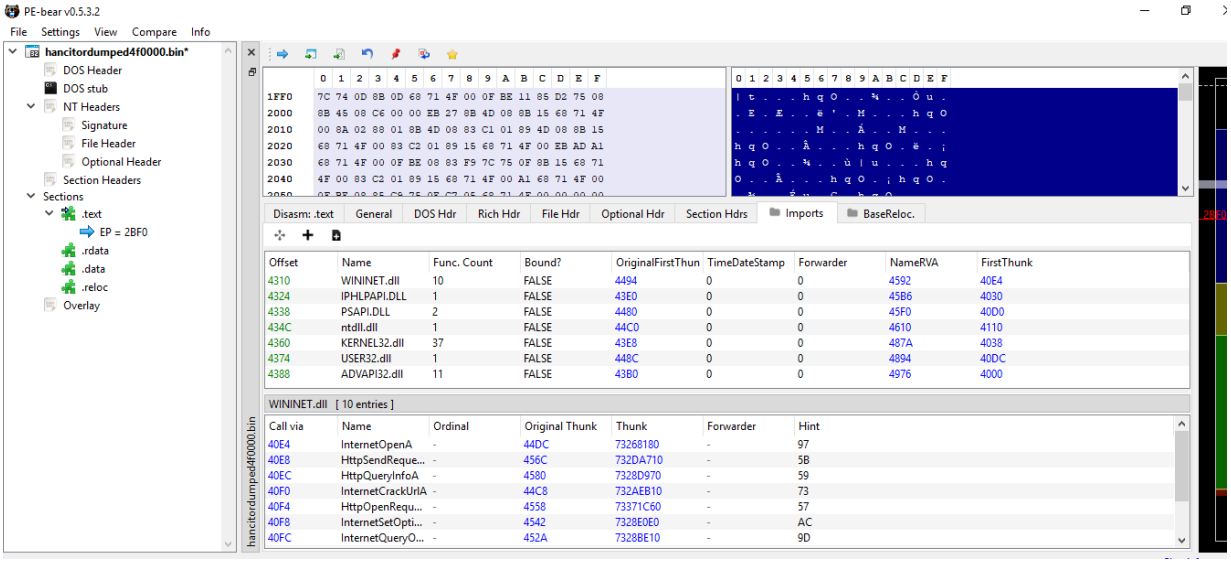
Here we have set the Raw Addr. Same as Virtual Addr. And now calculate Raw Size now make Virtual Size same as Raw size.



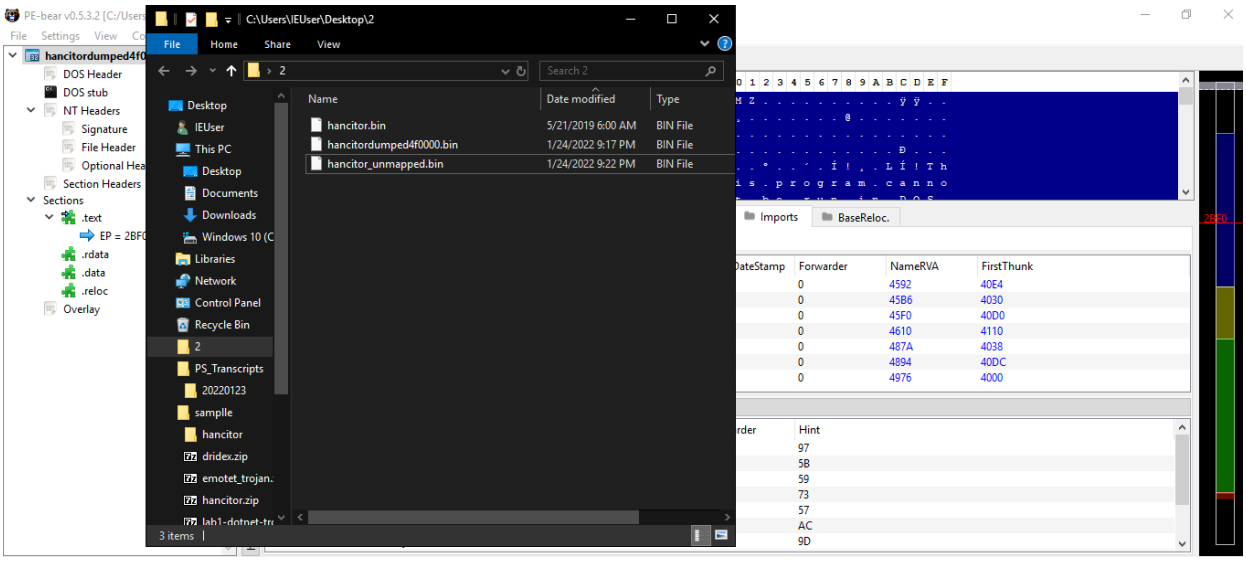
Now fix the image base in Optional Hdr. tab make it 4F0000.



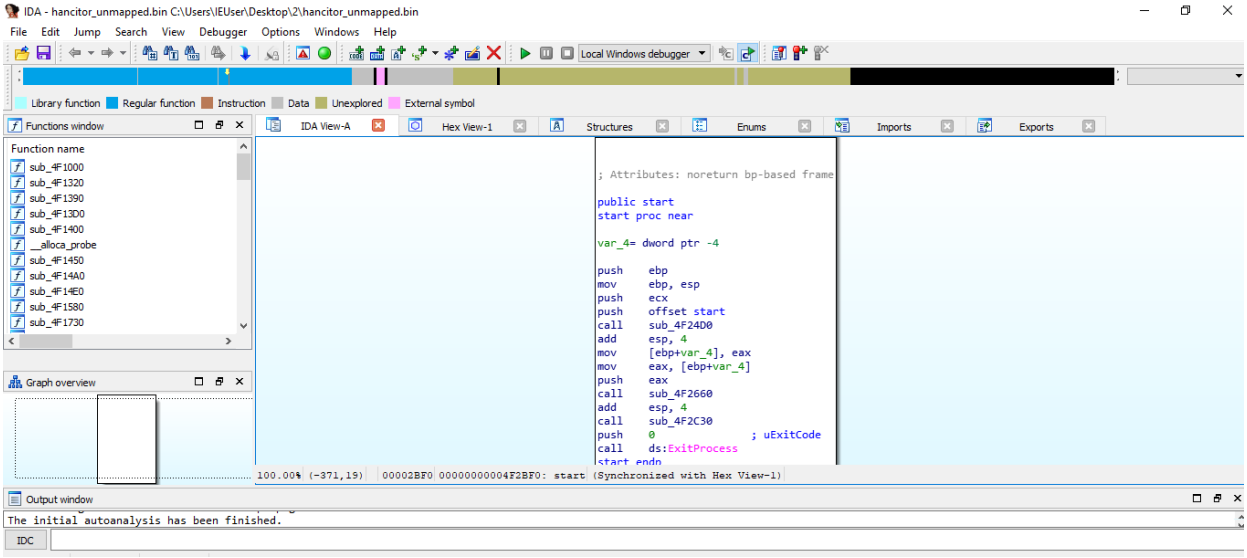
Now here we can check all the imports which are fixed now.



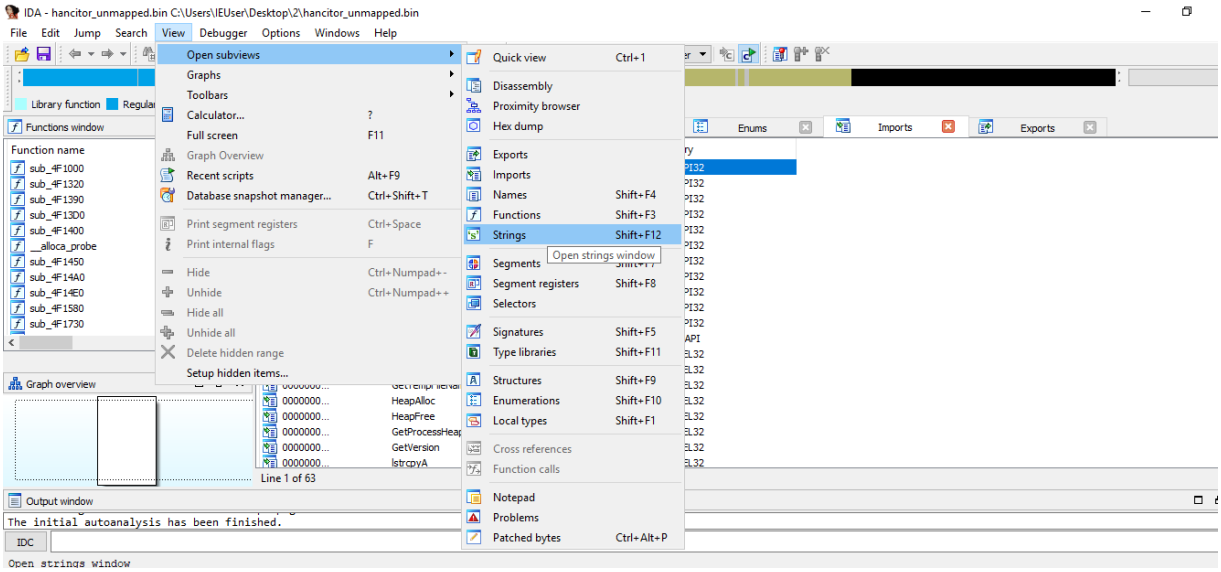
Save that file and load it in IDA .

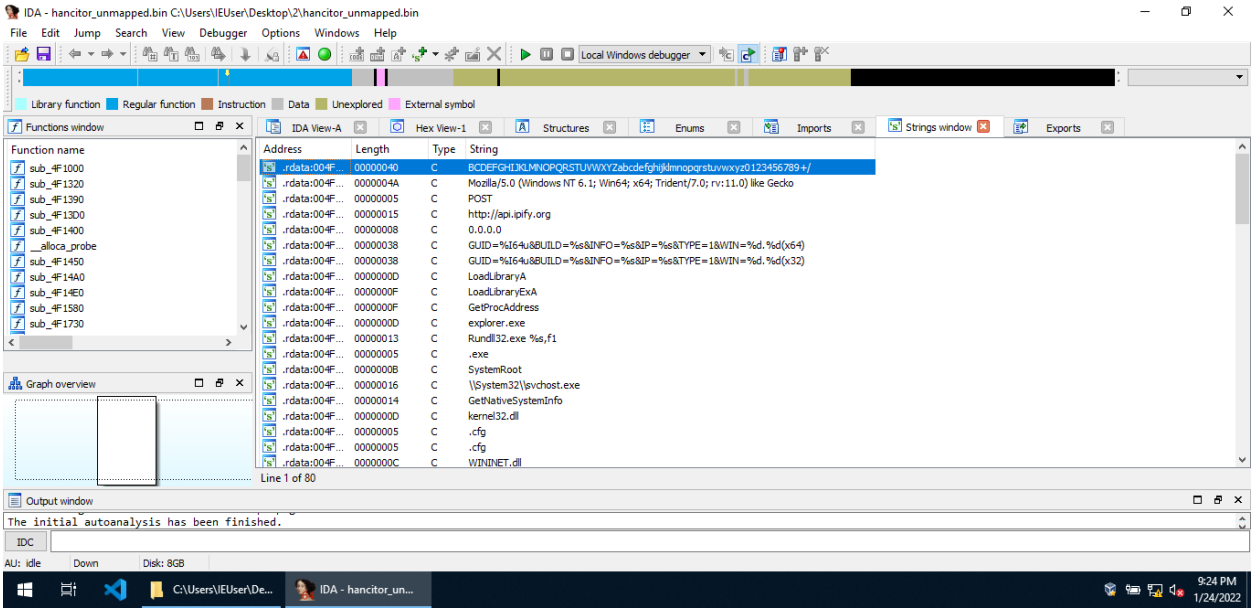


Now here we can see all the function name which were earlier not visible.



We can also view strings present in it.





So here we have successfully unpacked the malware using API Hooking method.