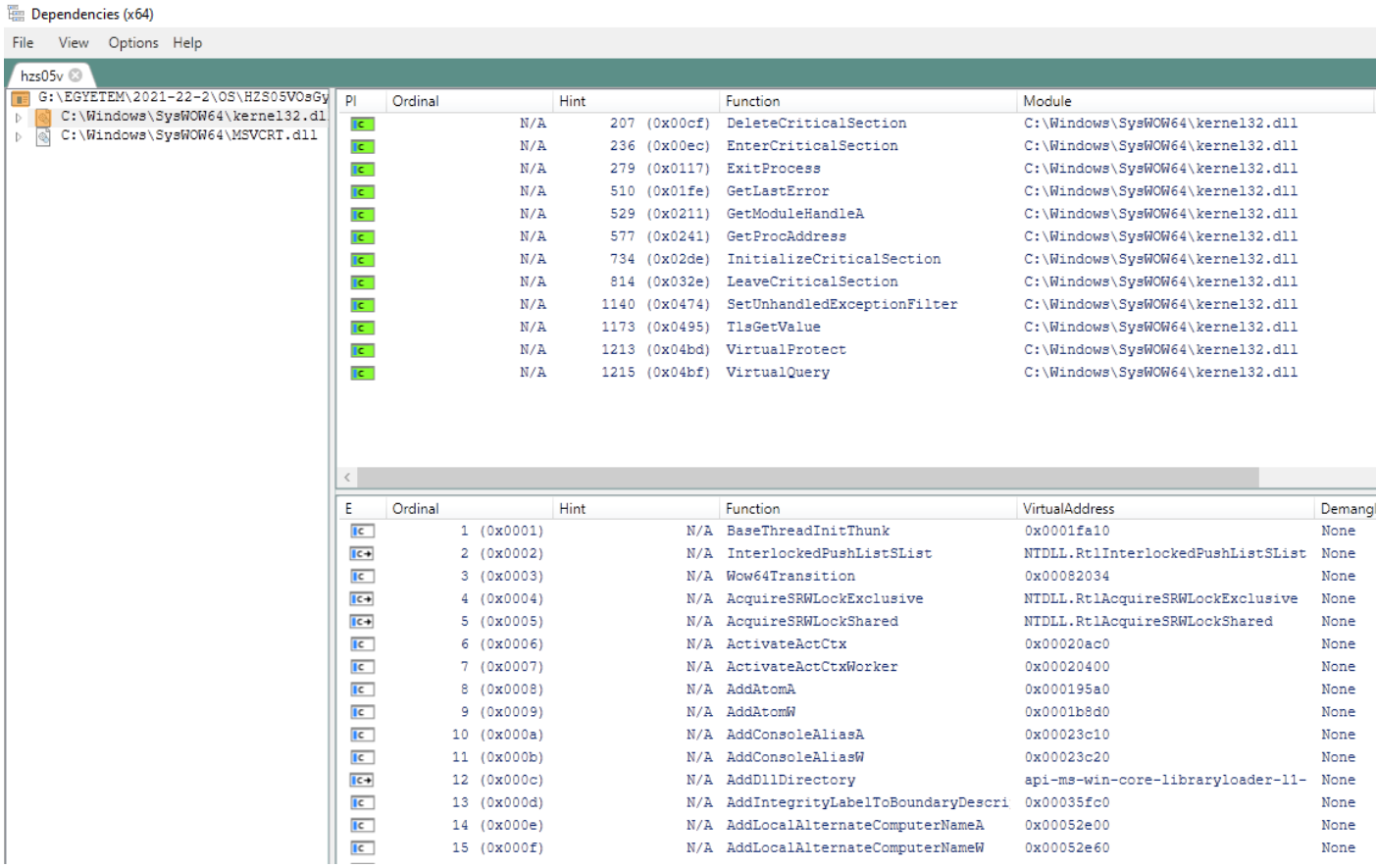
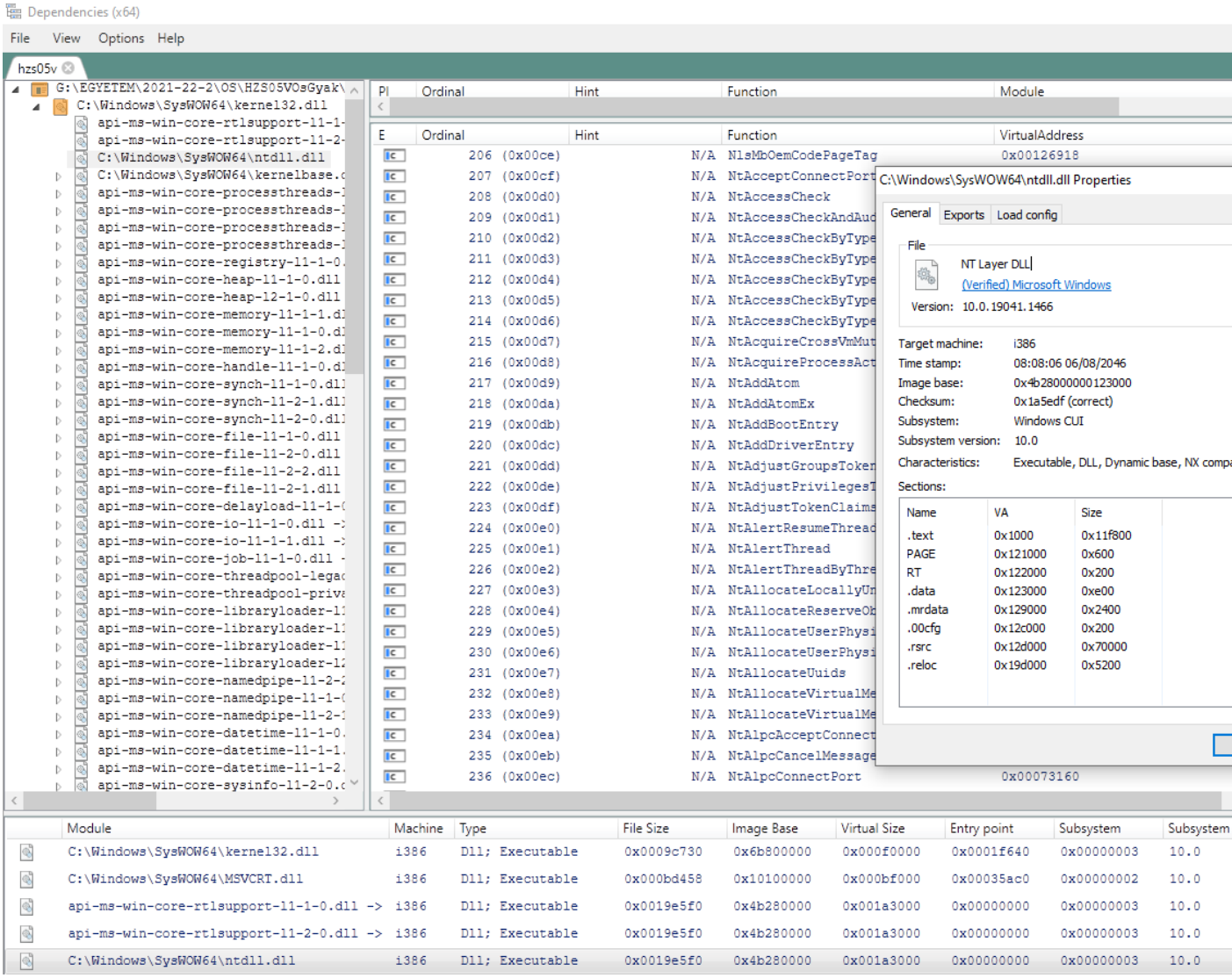
a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből (Win alrendszer DLL)!



b.) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról! „



Az NTDLL.DLL a Windows Native API-t exportálja, és ezzel nagyon sok függvényt képes használni. A natív API az operációs rendszer felhasználói módú összetevői által használt interfész, amelynek a Win32 vagy más API-alrendszerek támogatása nélkül kell futnia. Ennek az API-nak a nagy része az NTDLL.DLL ban van implementálva, és ezekben a könyvtárakban az exportáltak többsége Nt előtaggal rendelkezik, például az NtDisplayString. A natív API-kat a KERNEL32.DLL által exportált „kernel API” vagy „alap API” megvalósítására is használják. A Windows-alkalmazások nagy többsége nem hívja meg közvetlenül az NTDLL.DLL-t