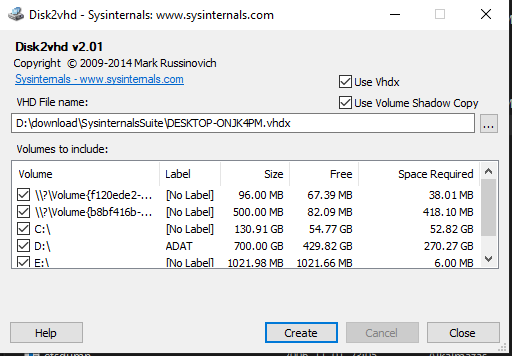
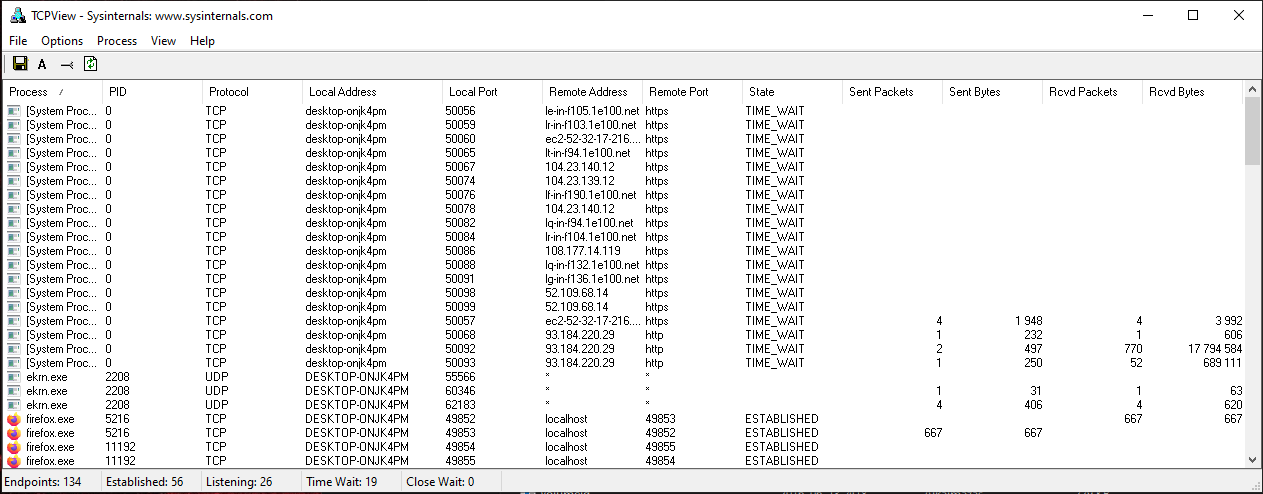
Szűcs Attila DJA75O

2. Operációs rendszerek gyakorlat

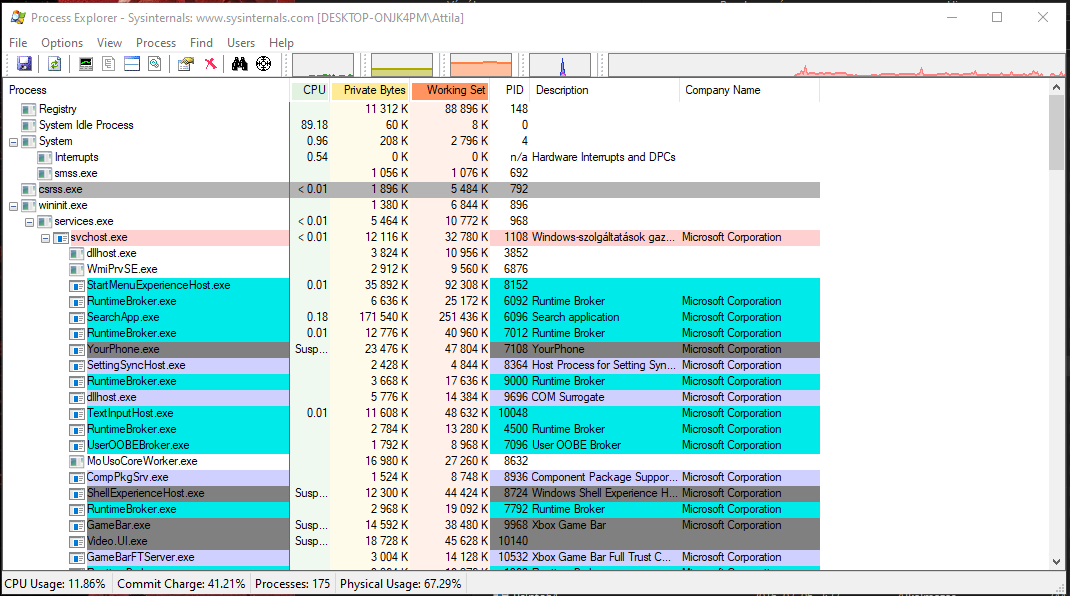
1. Letöltöttem a Sysinternals Suite.
2. a) A Disk2Vhd segítségével a fizikai lemezből lehet egy virtuális lemezt készíteni



b) A TCPView segítségével megtudjuk nézni a számítógépen lévő alkalmazások adat forgalmát

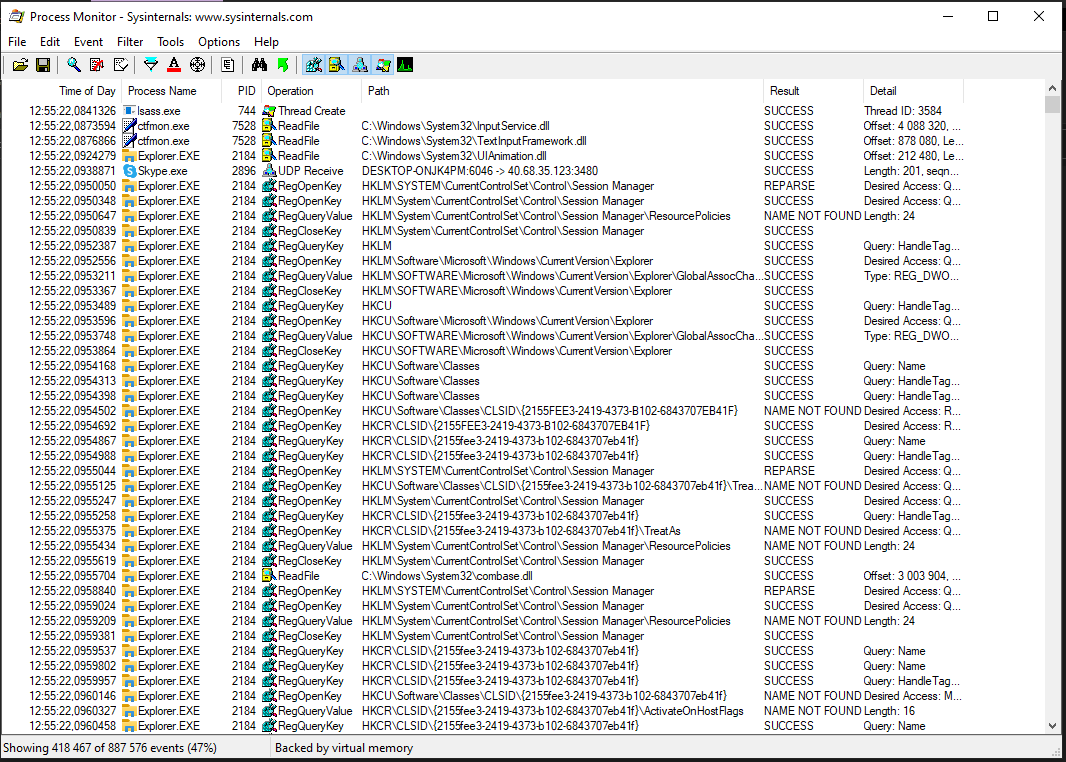


c) Process Explorer: segítségével meg nézhetjük a számítógépünk processzorának a terheltségét

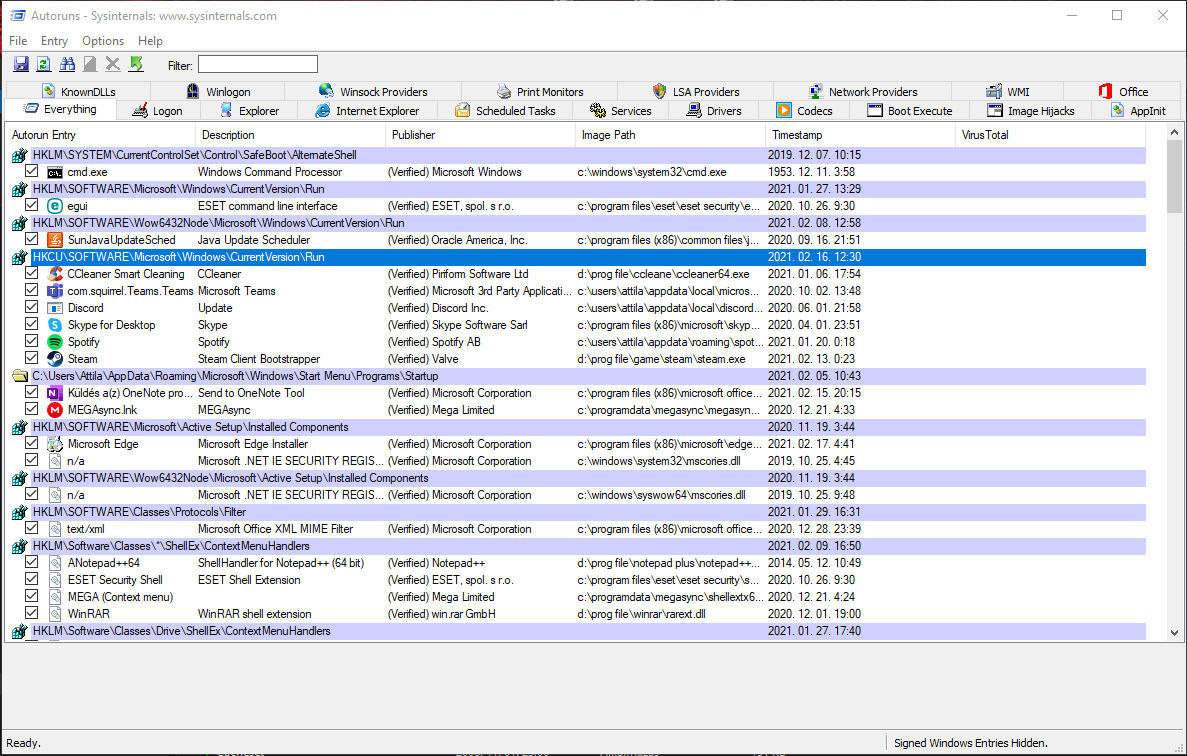


Process Monitor: Hasonló a Process Explorerhez de itt nem látjuk hogy az egyes programok

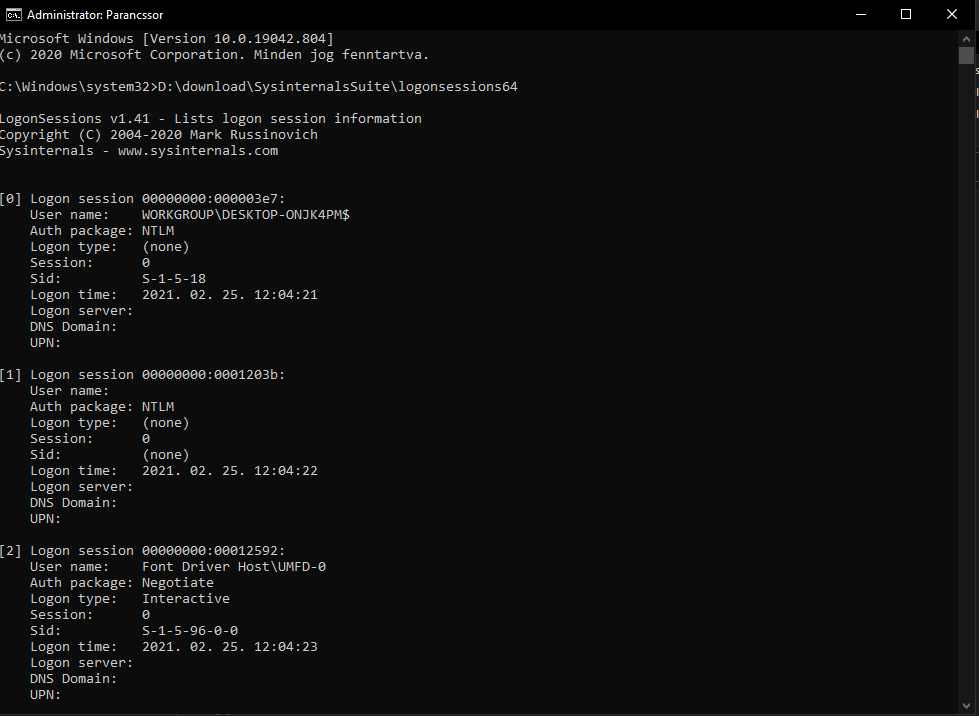
százalékosan menyire használják a számítógépünk proceszorát



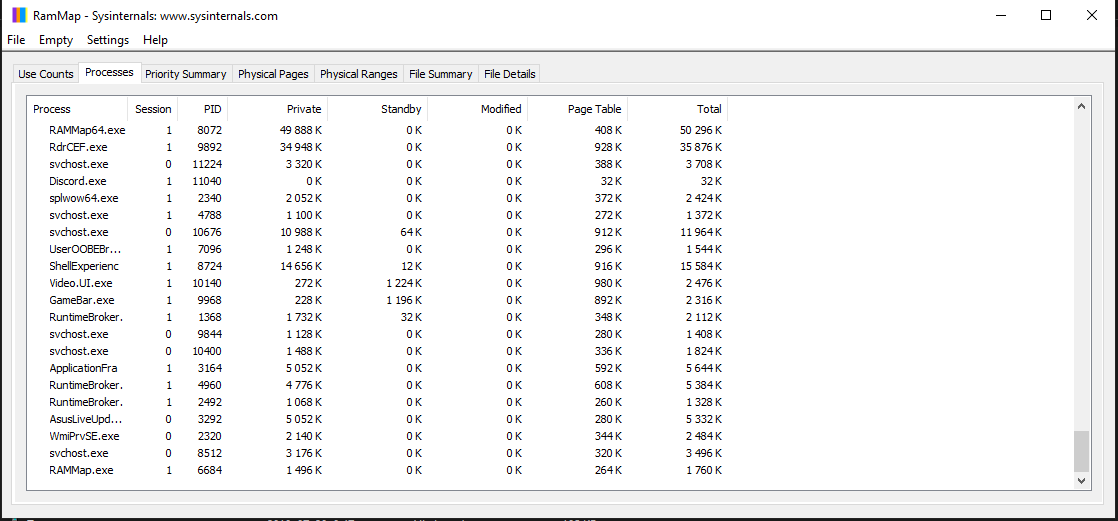
AutoRuns: A Windows környezetben történő automatikus futtatás vezérlés. A gépindításokkor

ez indítja el az automatikusan induló programokat illetve a harmadik féltől származó programokat

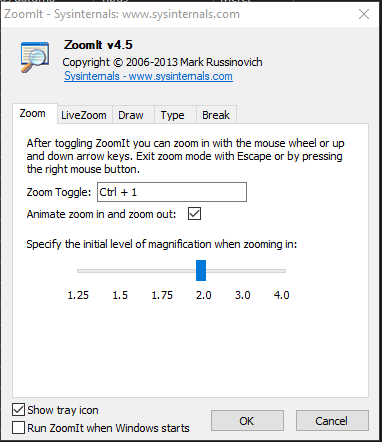
d) LogonSession: Segítségével megnézhetjük hogy mikor jelentkeztek be a számítógépinkbe



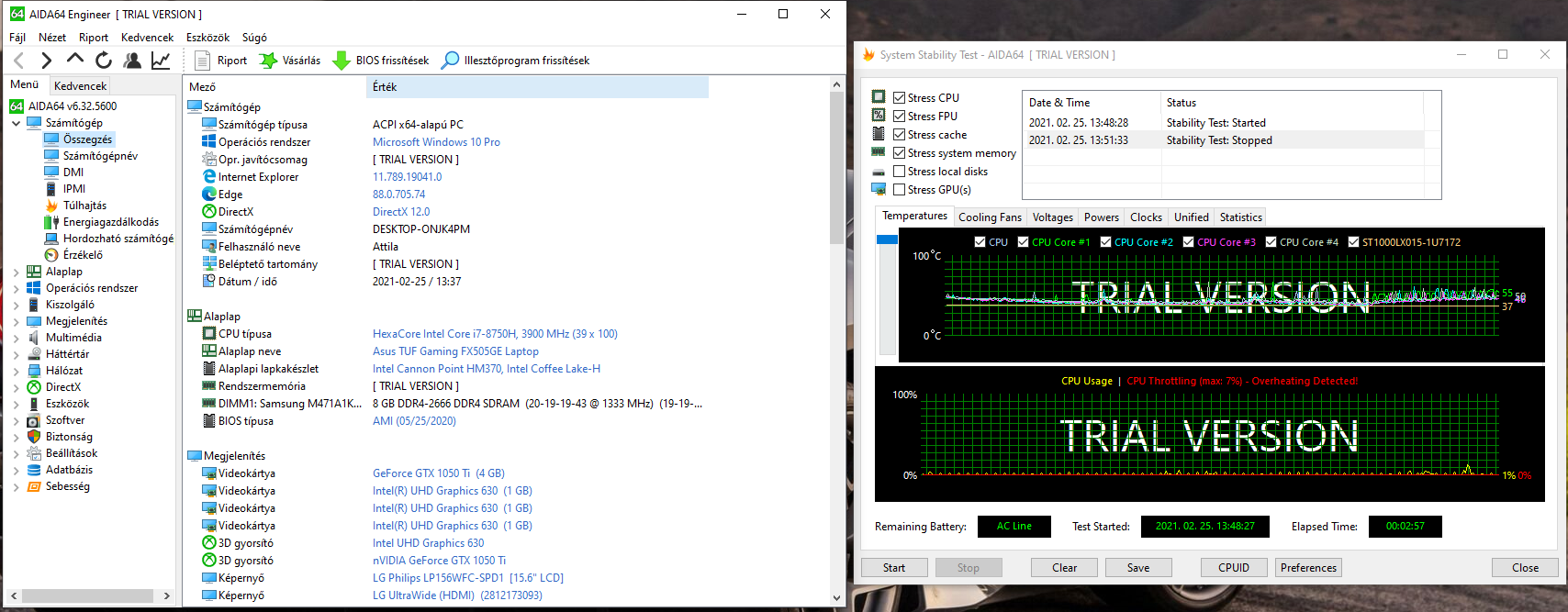
e) RAMMap: Segítségével megnézhetjük a számítógépünkben lévő ramnak a használtságáat



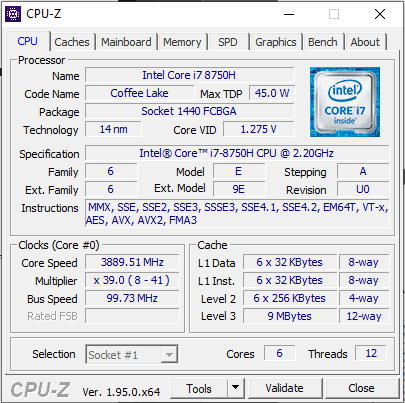
f) Zoomlt64: Segítségével bele nagyíthatunk a képernyőnkbe



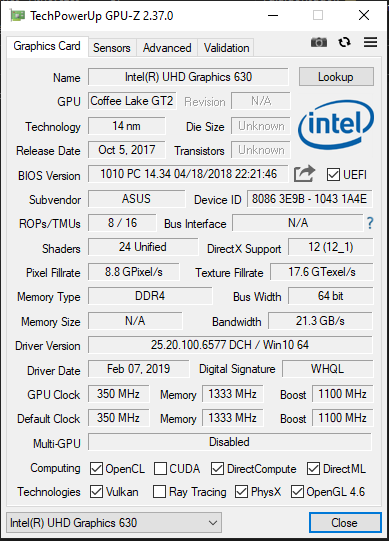
1. AIDA64: Segítségével megnézhetjük hogy a számítógépünkben milyen alkatrészek vannak és

végezhetünk egy stabilitás tesztet is

CPUZ: segítségével megnézhetjük a processzorunk tulajdonságait és montírozhatjuk is



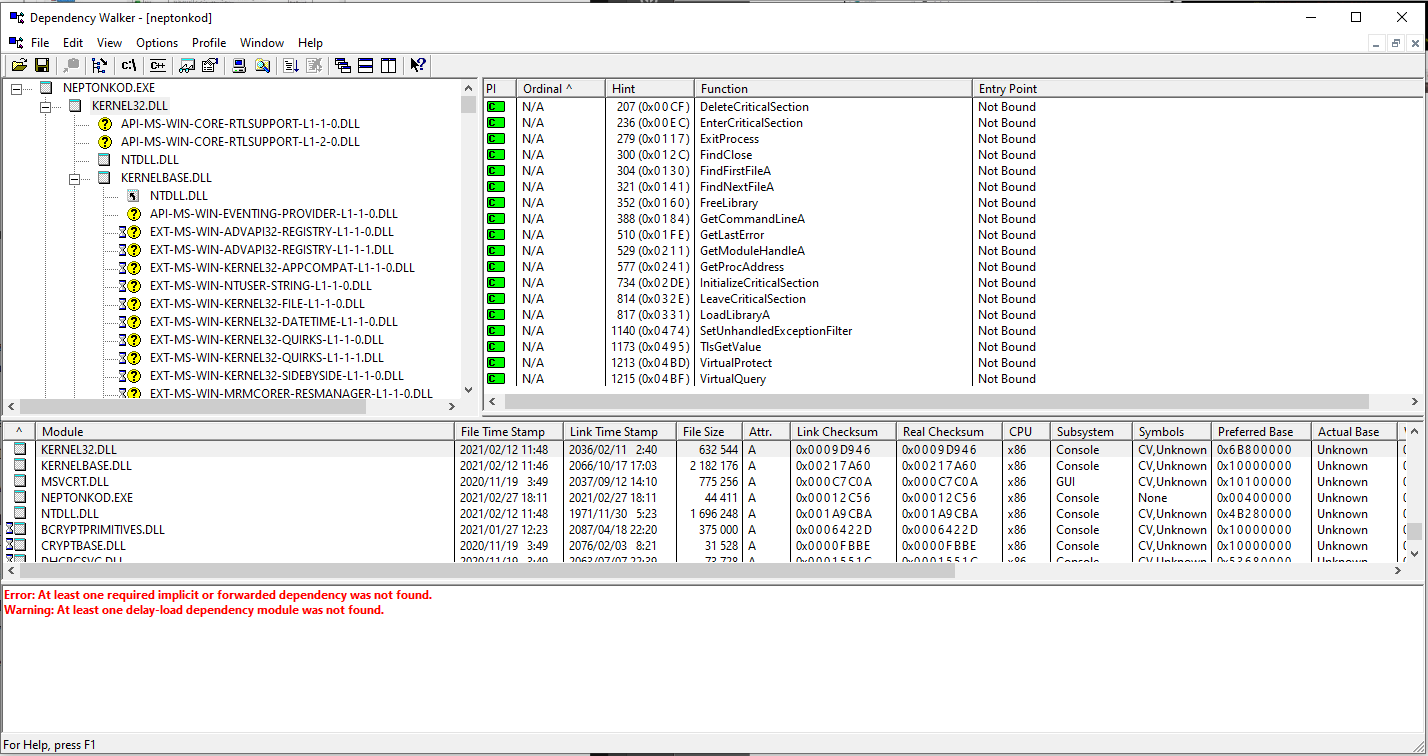
GPUZ: segítségével megnézhetjük a GPU tulajdonságait



1. a) A kernel32.dll a API-MS-WIN-CORE-RTLSUPPORT-L-1-0.DLL és a

API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL hívásokat használja

b) A kernel32.dll-nek az alábbi függőségei vannak:



c) Az NTDLL.DLL az a dinamikusan kapcsolódó könyvtár (Dinamically Linked Library – DLL), amin keresztül a felhasználói módú folyamatok elérhetik az NT-t. Mivel az egyes objektumok közötti kapcsolattartás az LPC mechanizmuson keresztül történik, így minden felhasználói objektum az NTDLL.DLL-en keresztül éri el a környezetét.

Az NTDLL által megvalósított működés egyszerű. Ha egy hívás érkezik, ellenőrzi a hívás paramétereit, és megvalósítja a user–kernel módváltást, majd meghívja az NT kért funkciót megvalósító függvényét.