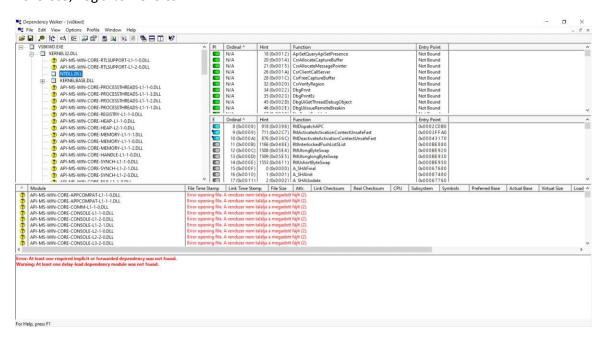
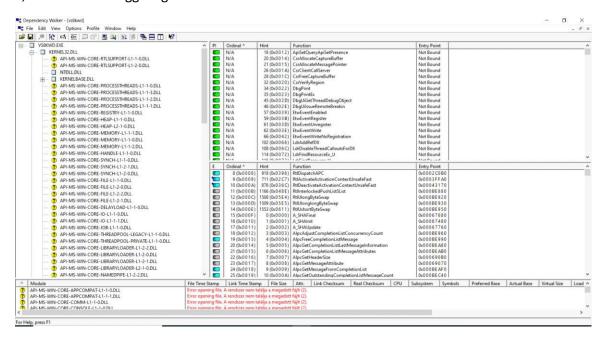
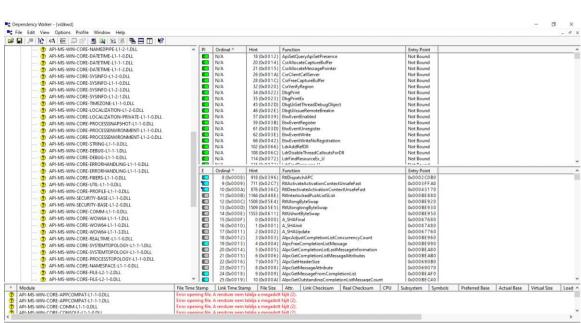
1, Memóriakezelés, Időkezelés, Stringkezelés, Fájlkezelés, Debug kezelés, Ki és bemeneti egységek kezelése, Regiszter kezelés



2, Windows API függőségei vannak a kernel 32-nek



3, Az NTDLL.dll a windows Natív API-ait tartlamazza. Ezek feladata hogy lefuttassa a lényeges processzeket a rendszer indításakor. Főképp vírusítrók alkalmazzák ezt a dll-t. Hozzáféréseket biztosítanak/törölnek ilyen pl a RtlAdjustPrivilege vagy Natív applikációkat futtatnak RtlCreateUserProcess vagy direkt leállítást végeznek NtShutdownSystem



For Help, press F1