Operációs rendszerek

BSc 3.gyak.

2021. 02. 24.

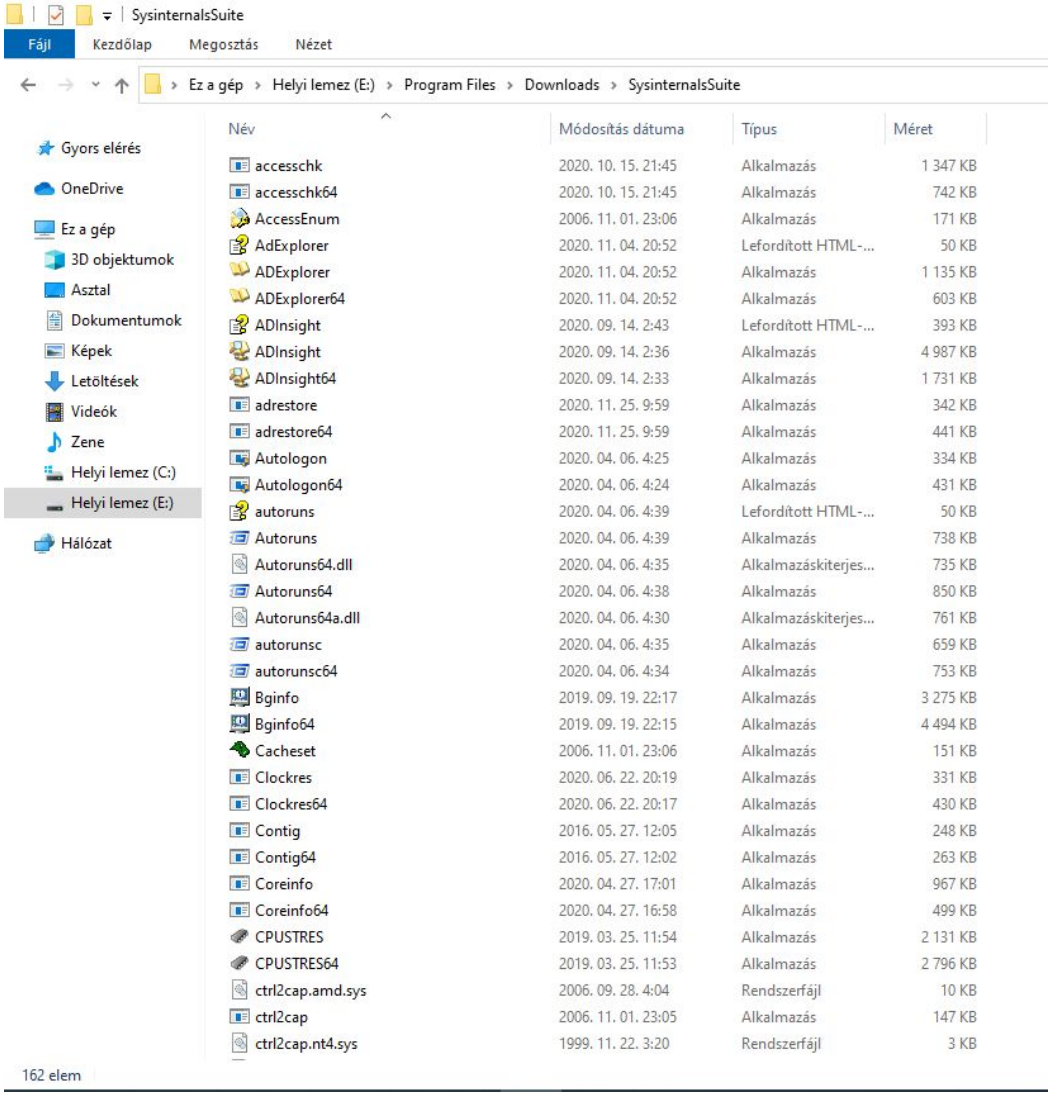
Készítette:

Kacsir András Bsc

Programtervező
VSG9L4

Miskolc, 2021

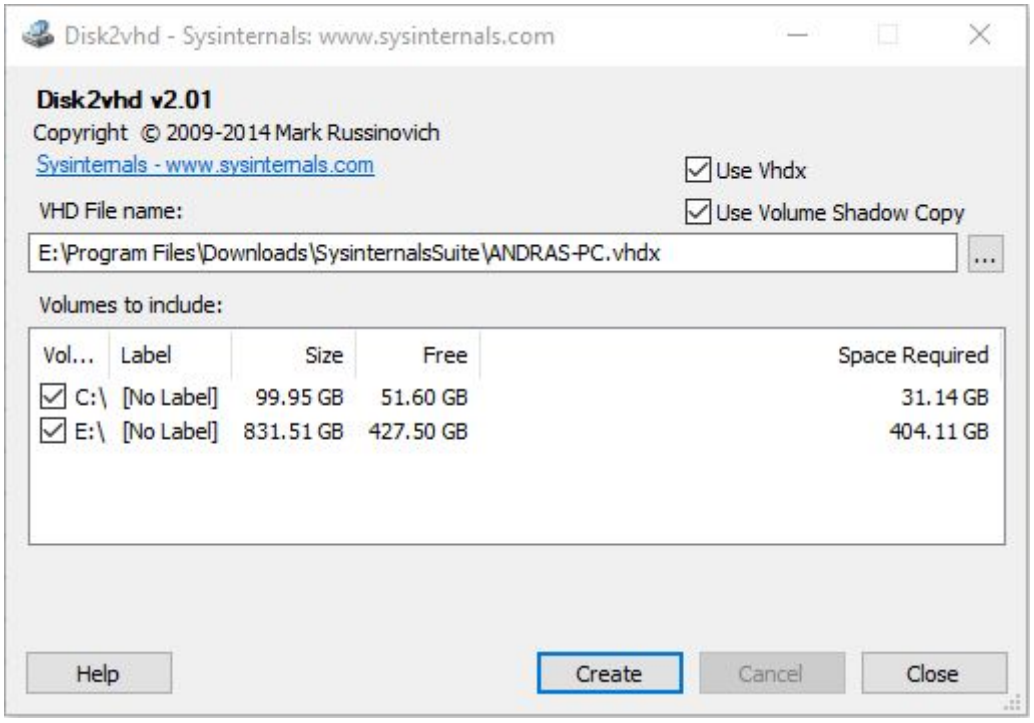
1. feladat – Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.kiírása Megvalósítás



letöltve

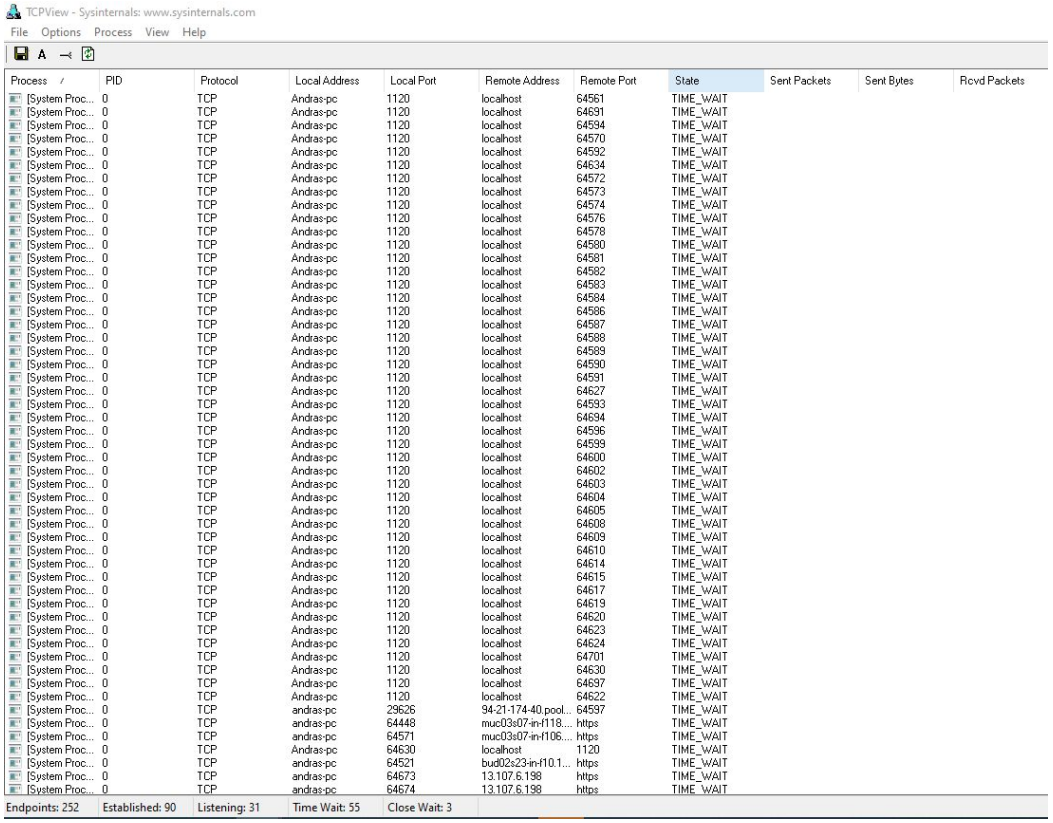
2. feladat - A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el:

a) File and Disk Utilities (Disk2vhd)



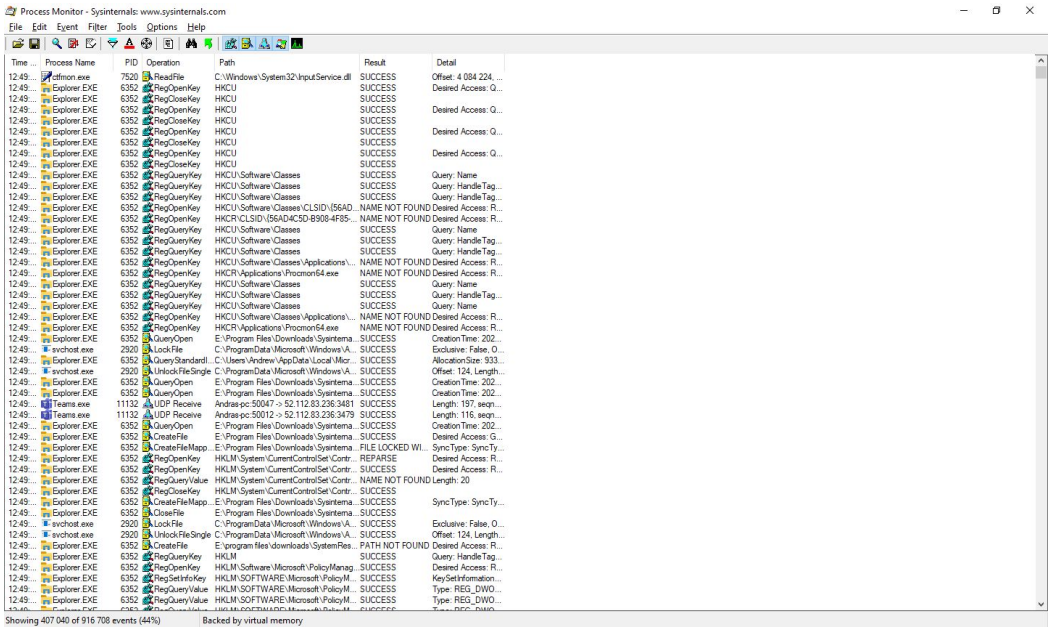
feladata hogy megnézze milyen meghatjóim vannak (C,E) és mennyi hely van rajta

b) Networking Utilities (TCPView)



Megmutatja az összes TCP and UDP végpontjait

c) Process Utilities (Process Explorer, Process Monitor, AutoRuns)

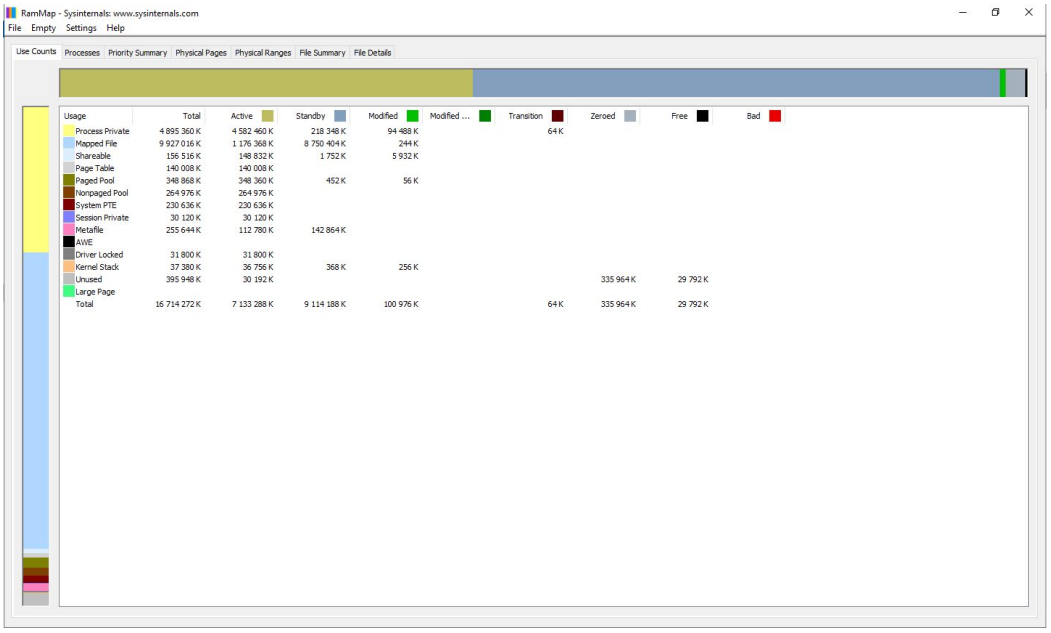


Megmutatja a registryket és a processzeket valós időben

d)Security Utilities (LogonSession)

elindult az exe majd rögtön bezárult így nem tudtam elindítani

e) Information Utilities (RAMMap)



Megmutatja hogy mennyi memóriát használnak az adott programok

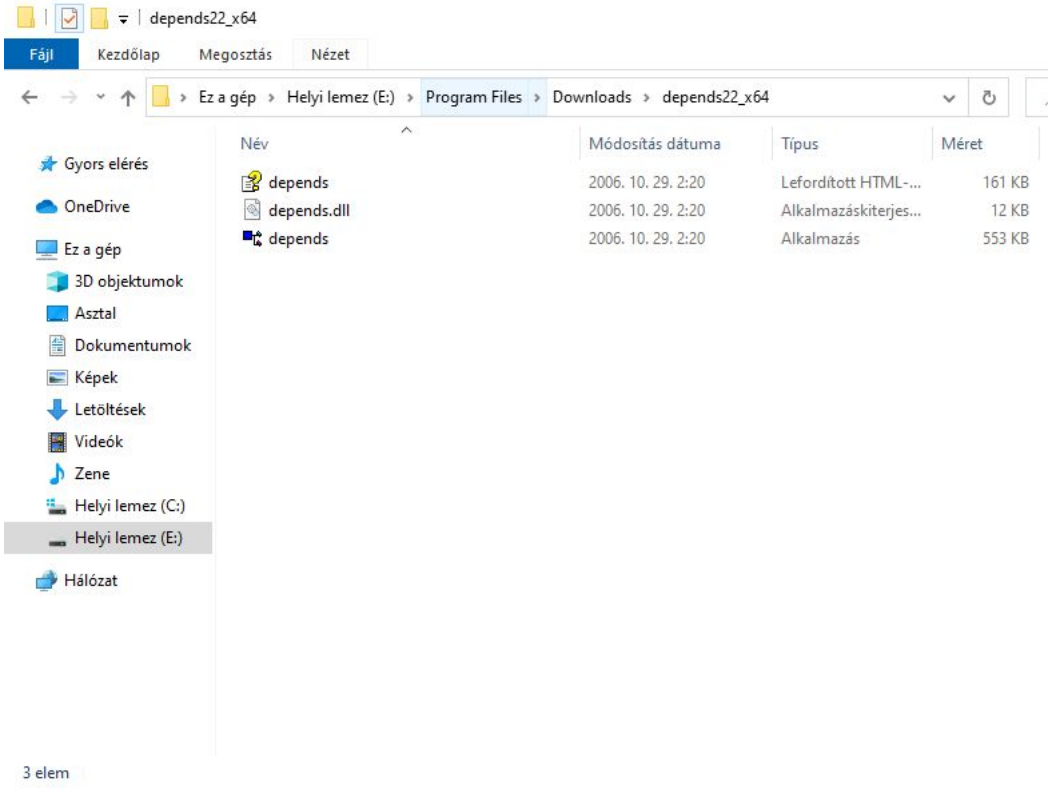
3. feladat - Töltse le és végezzen vizsgálatot az AIDA64_Engineer_v5.98.4800_Portable, CPU-Z, GPU-Z programokkal.

Nekem már lent volt és el is használtam a 30 napon trialomat

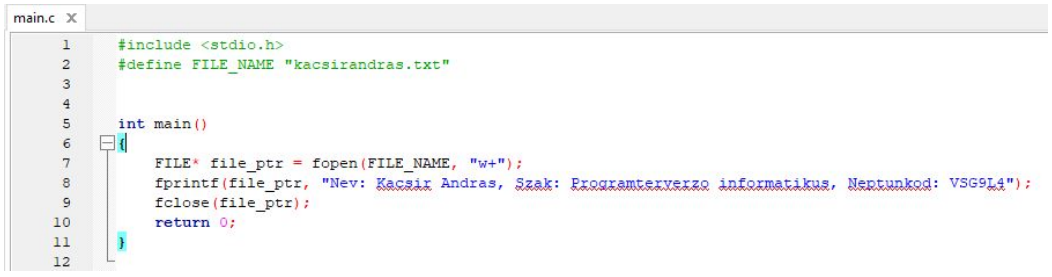
4. feladat - Töltse le a következő programot: Dependency Walker

URL: http://www.dependencywalker.com/

Feladata: a segédprogram megvizsgálja milyen könyvtárakra, és azon belül milyen függvényekre hivatkozik egy elindított program.



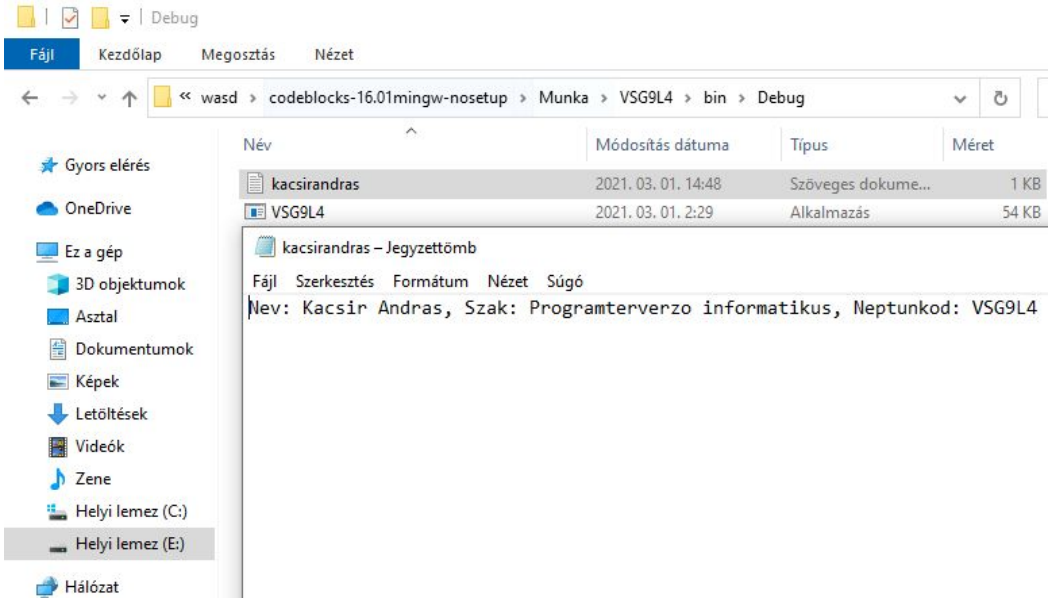
Készítsen egy neptunkod.c nevű forráskódot, amely egy vezeteknev.txt fájlt létrehoz, olvas,
majd bezár. Tartalma: Név, Szak, Neptunkod etc.



Fordítsa le kódot a C fordító, amely létrehoz egy objektum kódot,

ezután egy linker

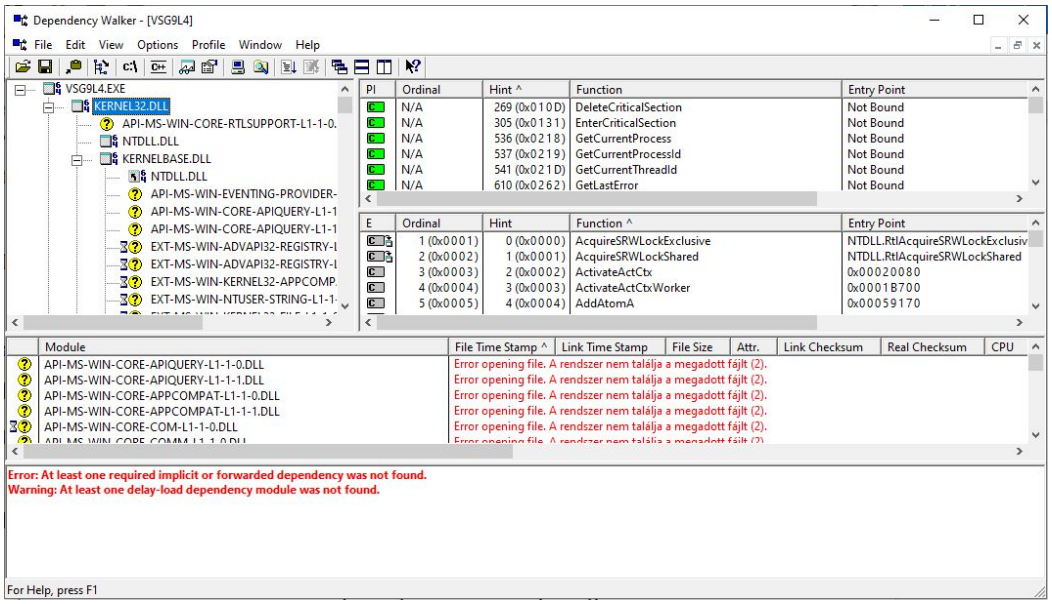
segítségével készítsen egy végrehajtó állományt: neptunkod.exe



A Dependency Walker segítségével végezze el a következő feladatokat.

Nyissa meg a neptunkod.exe fájlt!

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



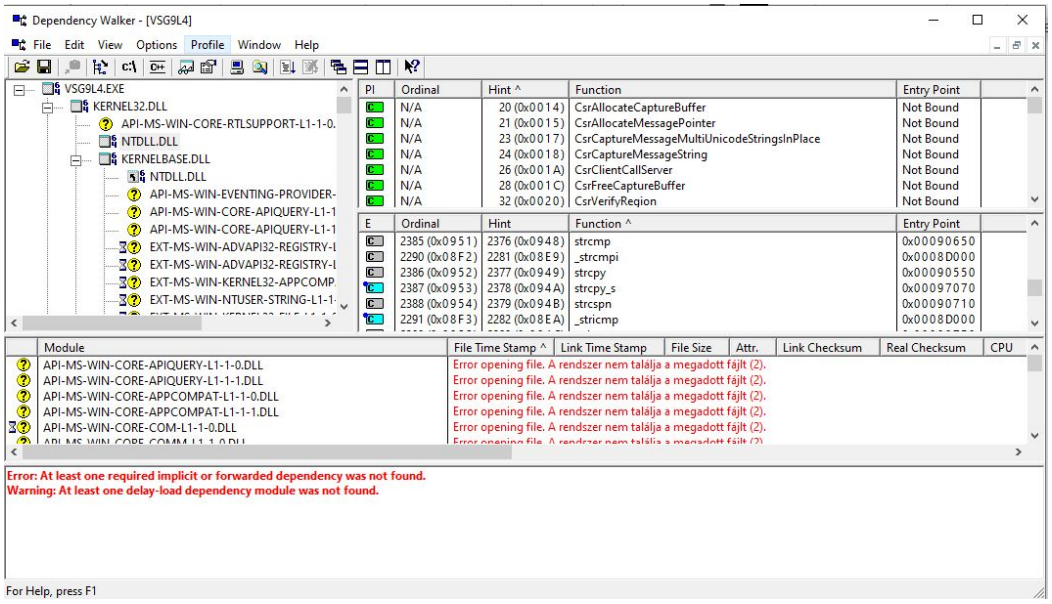
Api hívás például API-MS-WIN-CORE....

b.) Milyen függőségei vannak a kernel32.dll-nek!

felül az import és alul az export függvények

c.) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált

függvényeket, milyen információkat kap az NT API-ról!



Felhasználta a program az strcpy parancsot ami c nyelvben megtalálható parancs