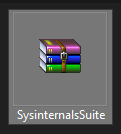
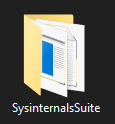
***Operációs Rendszerek BSC***3. gyakorlat  
2021.február 24.

**Készítette:**Kércsi Bence  
Programtervező Informatikus  
ILVIYV

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

<https://docs.microsoft.com/hu-hu/sysinternals/downloads/sysinternals-suite>

Letöltést követően ez a tömörített file jelent meg, amit aztán kicsomagoltam:



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

**a) File and Disk Utilities (Disk2vhd)**

**b) Networking Utilities (TCPView)**

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

**d)** Security Utilities (LogonSession)

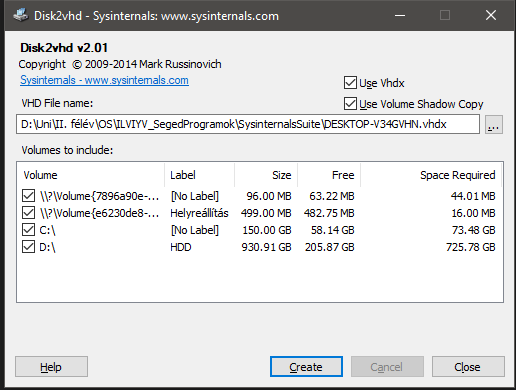
**e)** Information Utilities (RAMMap)

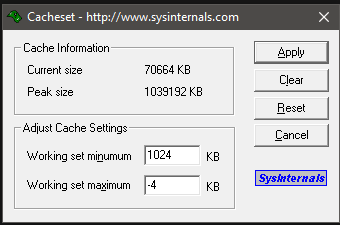
A felsorolt eszközök közül minden eszköz esetén töltse le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét egy-egy mondattal - majd mentse el a megadott dokumentumba (képernyőkép).

*Megj:* a zárójelben lévő eszközön felül válasszon még egy eszközt is.

A, File and Disk Utilities:

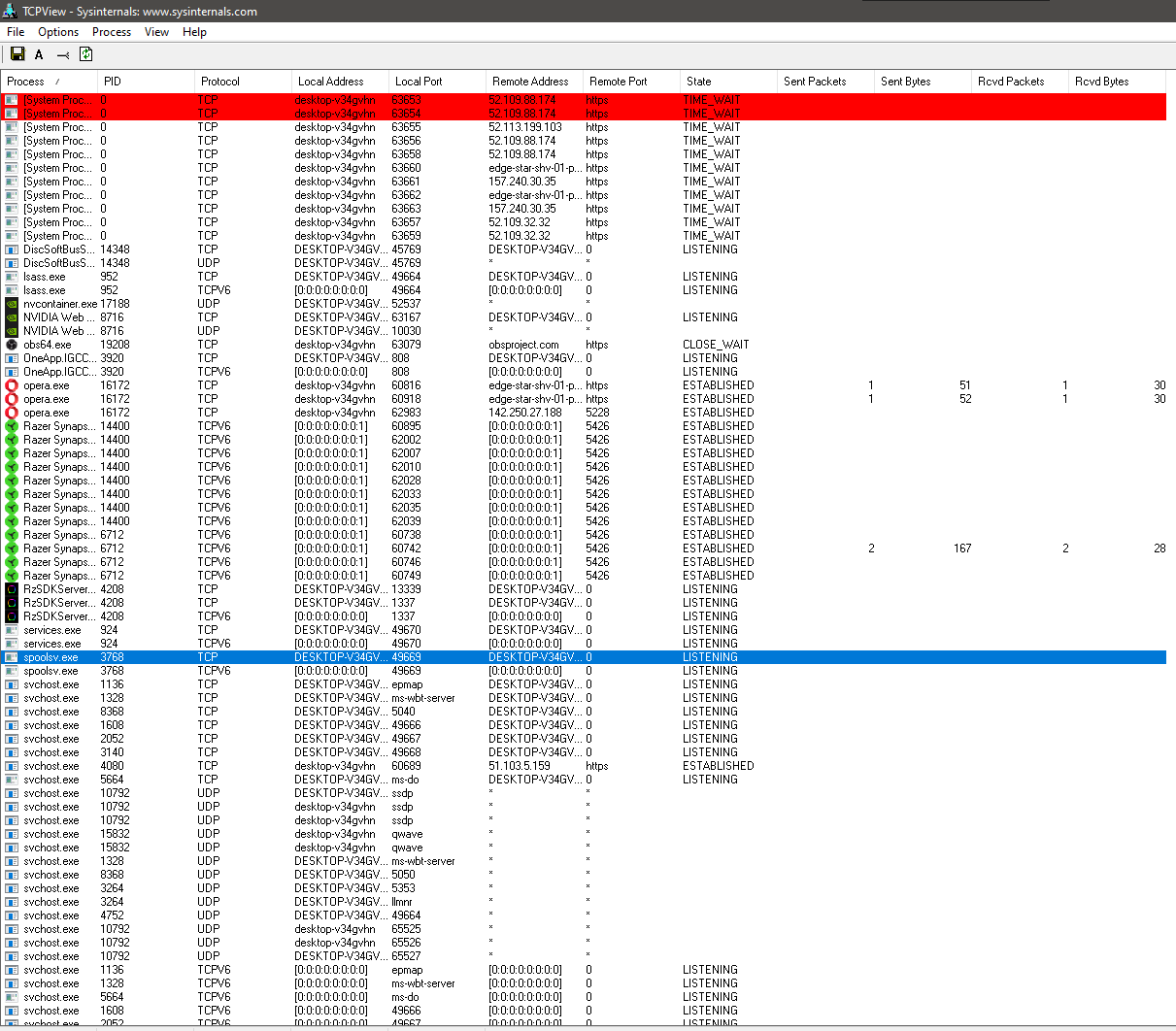
Disk2vhd:

  
Kilistázza jelenleg milyen partíciókra van osztva, ezeknek mennyi a limitjük, illetve virtuális merevlemezt tudunk vele létrehozni.  
Cacheset:

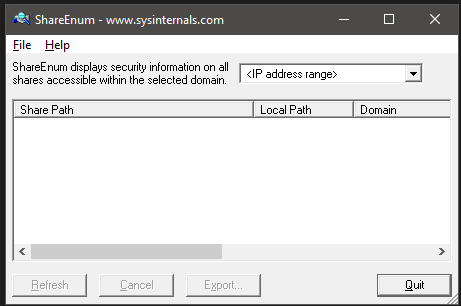


Tudjuk vele állítani a cache méretét.

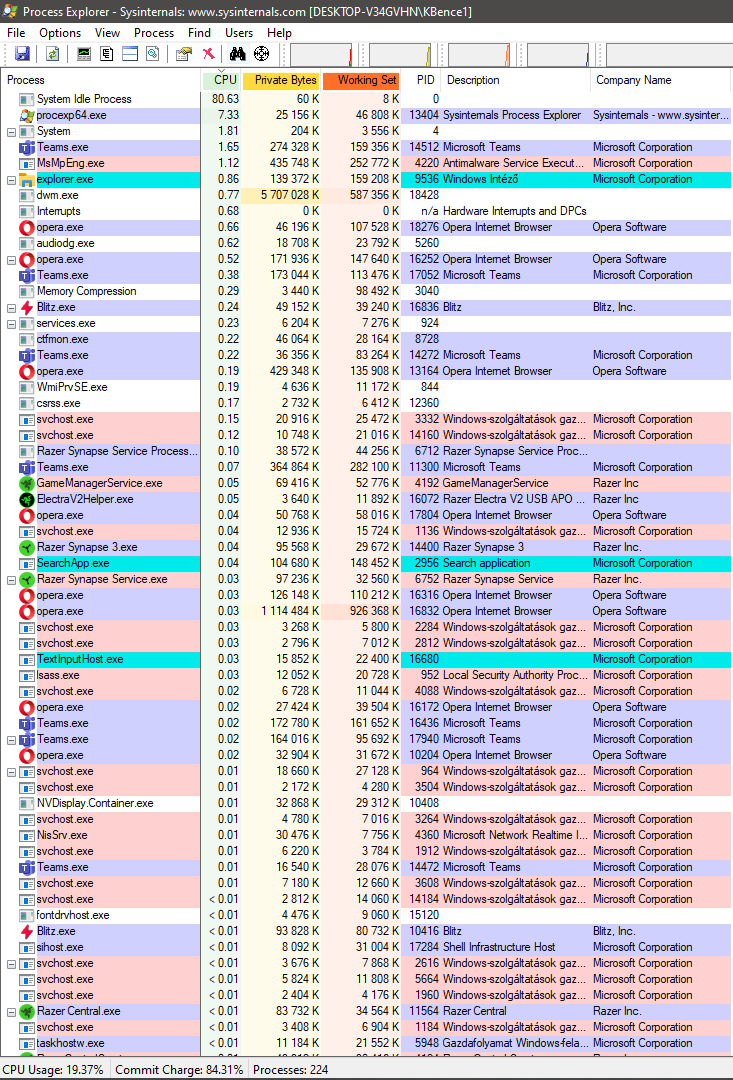
B, Networking Utilities:

TCPView:  


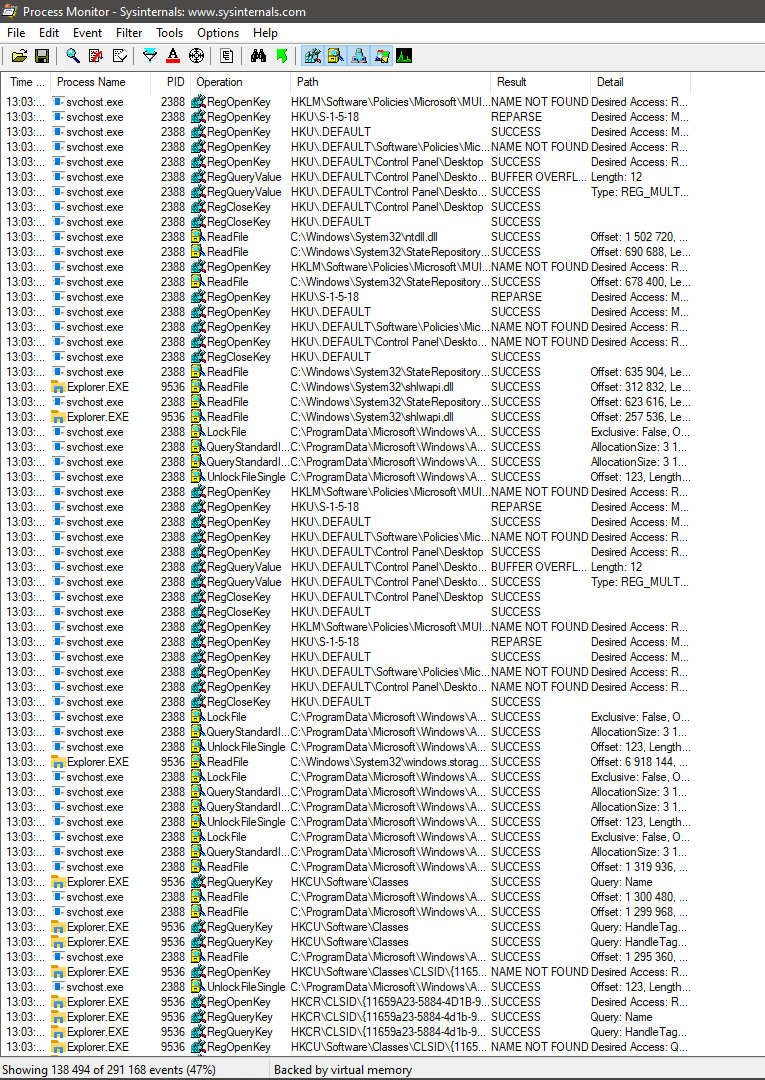
Kilistázza részletesen, a TCP és UDP kapcsolatok végpontját, az azokat használó processzek nevét, és címét.   
ShareEnum:



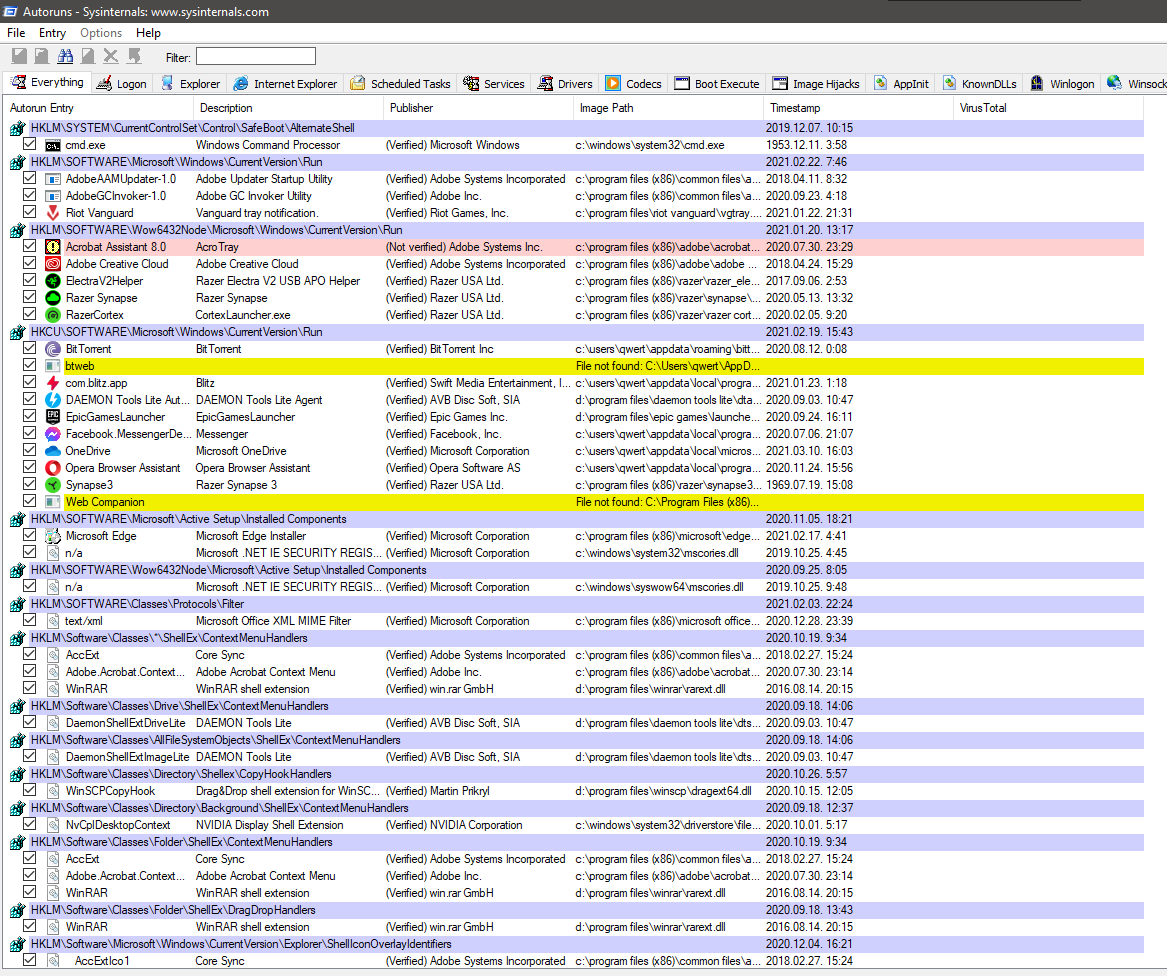
A hálózathoz csatlakoztatott gépek közt lehetséges vele megnézni „megosztott” fileokat. Részletesebben nem tudom bemutatni ugyanis nem csatlakozok olyan hálózathoz amiben ez lehetséges lenne.C, Process Utilities:

Process Explorer:

Megmutatja, hogy milyen DLL processzek futnak vagy vannak betöltve. Láthatjuk a processzek nevét, a CPU használatukat, egy rövid leírást, ahol van ott gyártó/tulaj nevét.

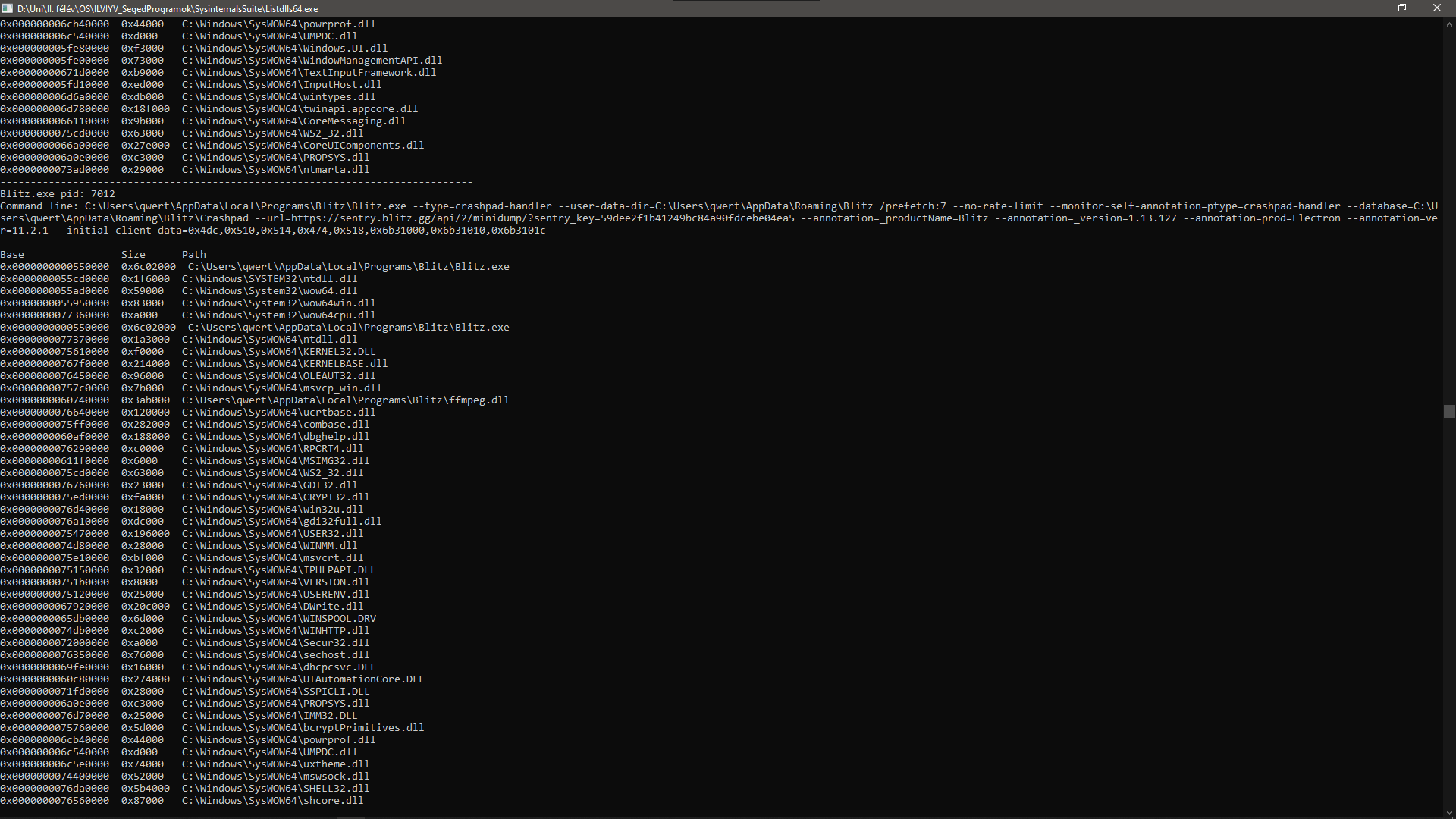
Process Monitor:  
  
Itt futó processzek nevét láthatjuk, elindulásuk idejét, feladatukat, elérési útjukat

AutoRuns:



Ez az automatikusan gép indítással induló processzeket listázza ki, indulásuk helyét, egy rövid leírást ad róluk, gyártójukat.

ListDDL:



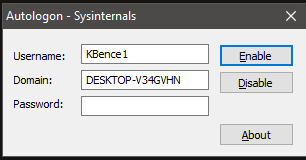
Kilistázza az elindított vagy beöltött DLL-eket.

D, Security Utilities:

LogonSession:

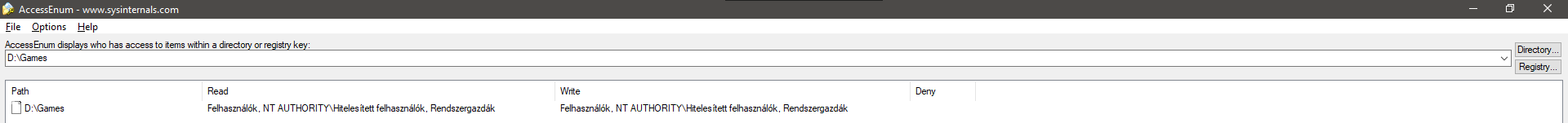
Valamilyen oknál fogva akár milyen módban próbáltam indítani nem indul.

AutoLogon:



Azt lehet megvalósítani vele, hogy egy adott felhasználói fiókba automatikusan belépjen, ha megadjuk az ahhoz tartozó helyes felhasználónév, jelszó kombinációt.

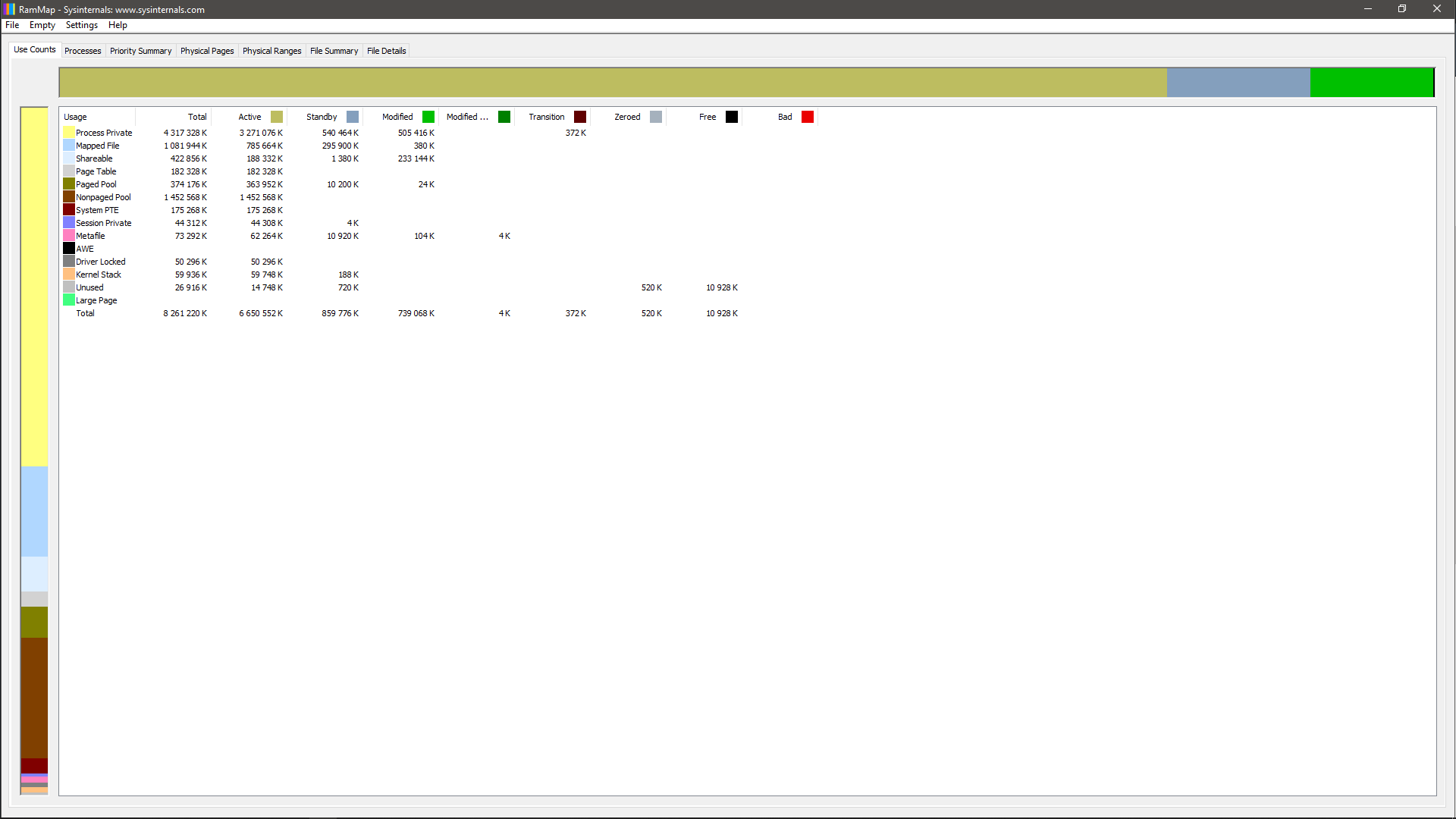
AccesEnum:



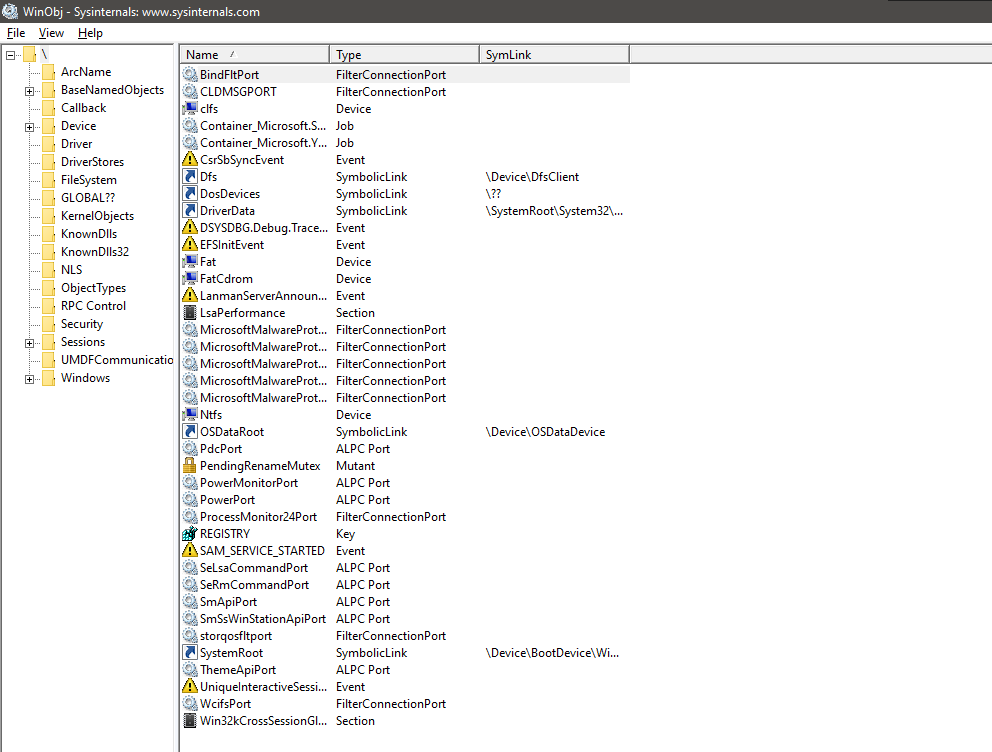
Megmutatja egy adott mappába melyik felhasználó csoportoknak milyen jogosultságaik vannak.

E, Information Utilities:

RAMMap:



Megmutatja, hogy mennyi RAM-ot használ a kernel illetve a driverek. Fizikai memóriáról is több információt is nyújt.Winobj:

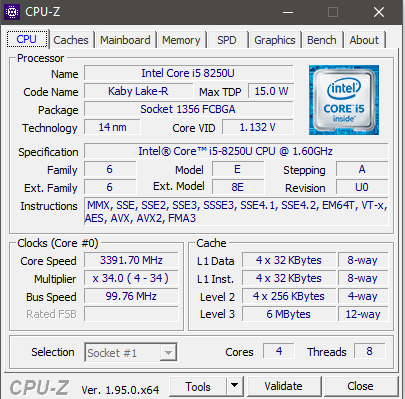


Megmutatja az objektumokkal kapcsolatos információkat. Jó réskeresésre is a biztonsági rendszerben.

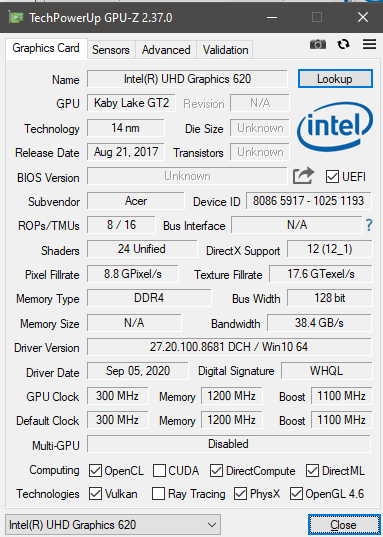
**3.** Töltse le és végezzen vizsgálatot az *AIDA64\_Engineer\_v5.98.4800\_Portable, CPU-Z, GPU-Z* programokkal.

A felsorolt segédprogramoknak írja le a szolgáltatásait és a futtatás eredményét egy-egy mondattal - majd mentse el az alábbi dokumentumba (képernyőkép is).

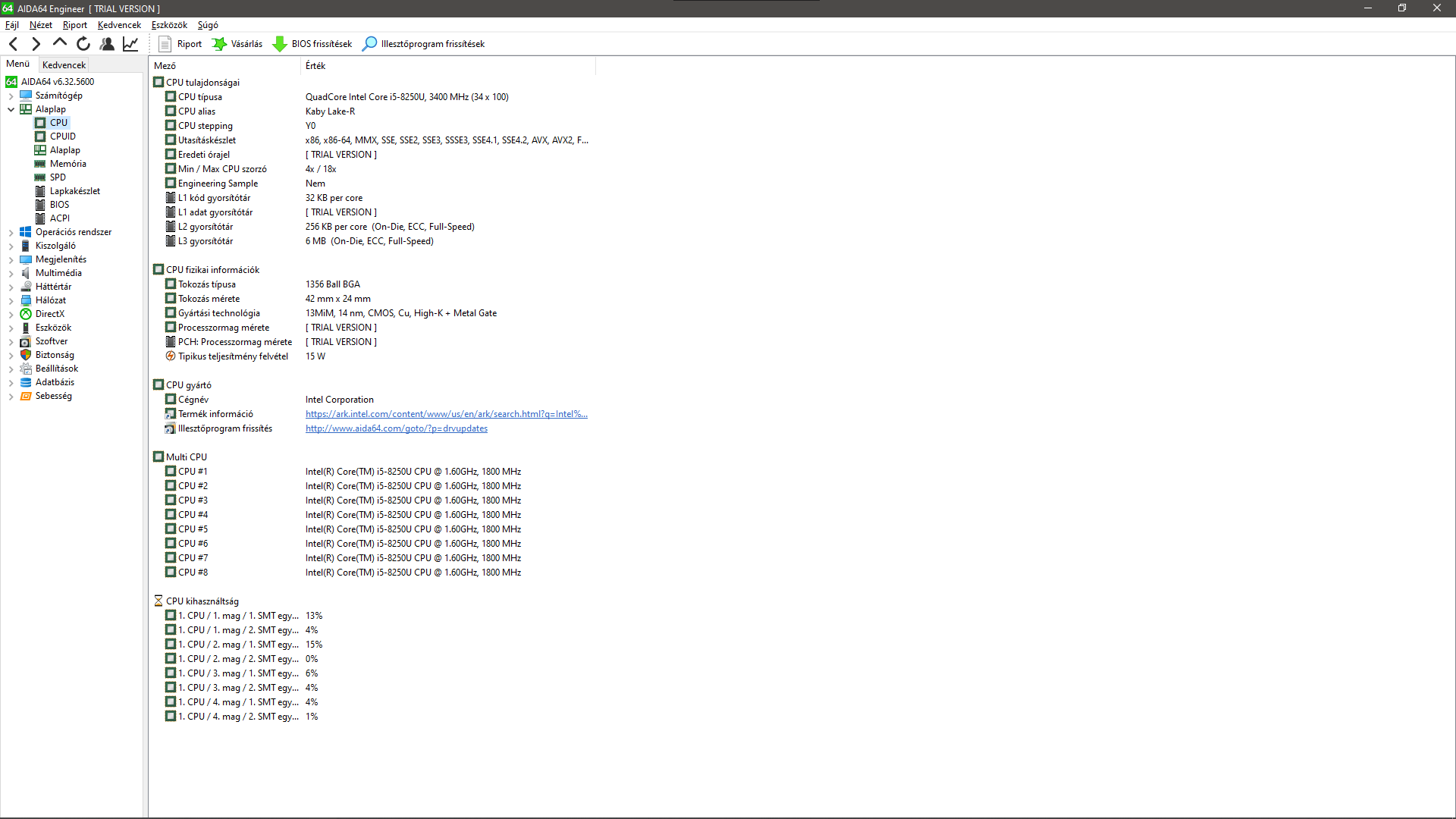
CPU-Z:



Információkat tartalmaz a CPUról. Milyen CPU van benne, hanyadik generációs, milyen órajelű, milyen teknológiával készült, ileltve további információkat is nézhetünk vele, például alaplap, memória, gpu stb.GPU-Z:



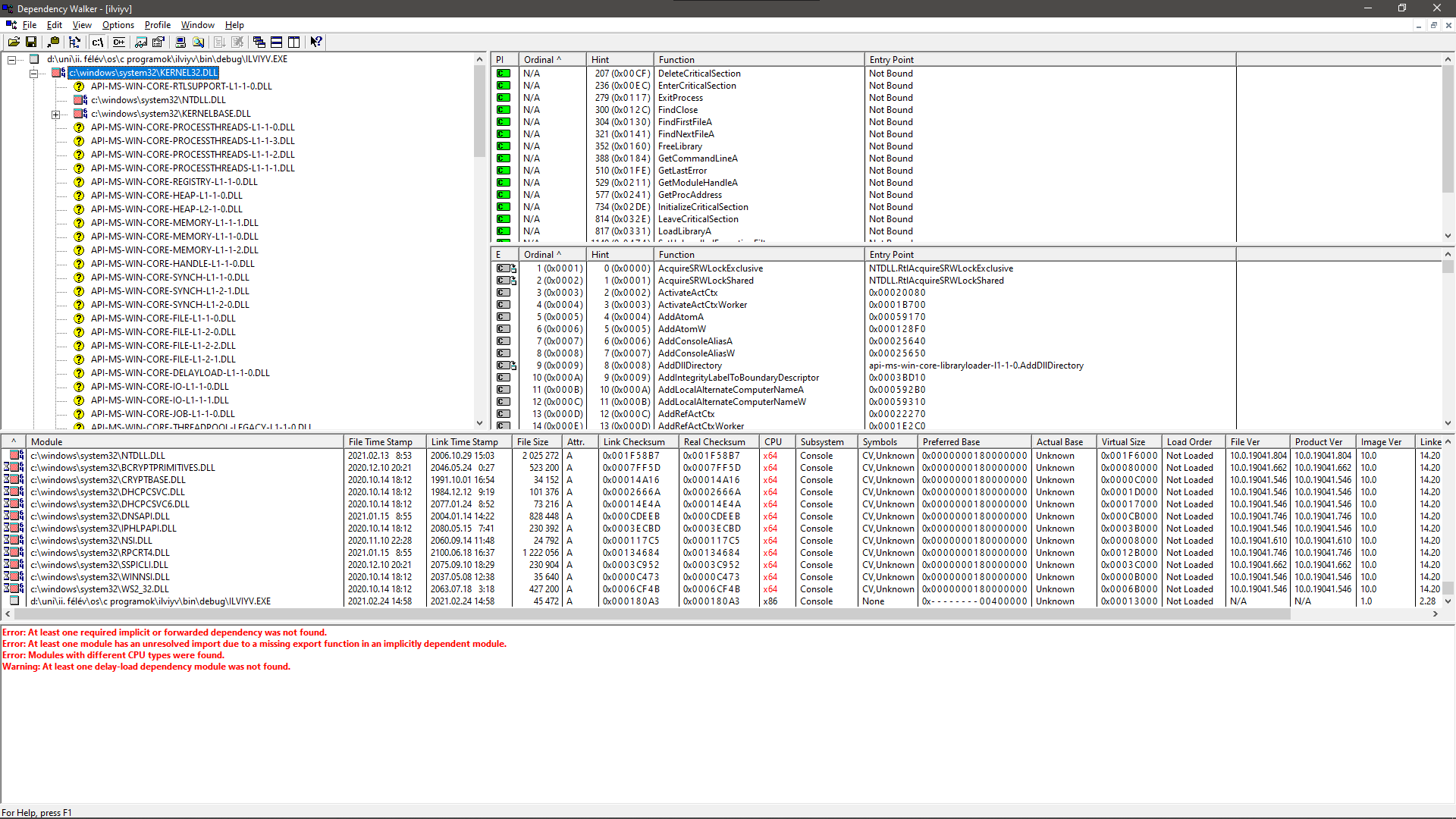
Részletesebb információkkal szolgál a GPU-ról. Milyen típusú, milyen teknikával készült, kiadásának ideje stb.AIDA:



Nagyon részletes leírást ad minden bal sávban felsorolt elemről.

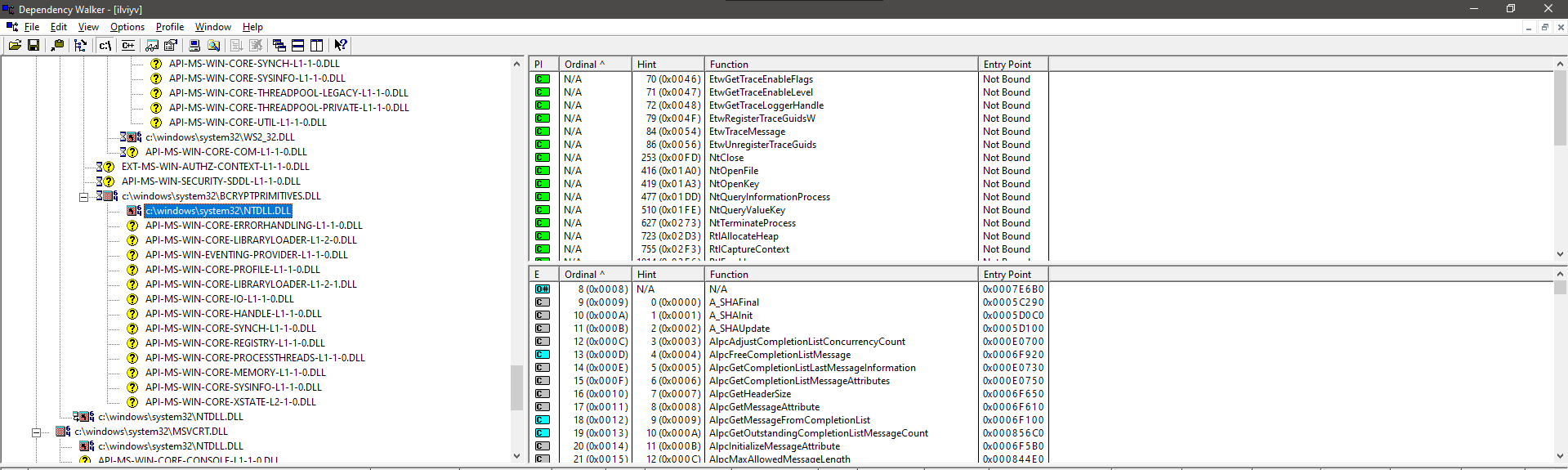
**4.** Töltse le a következő programot: Dependency Walker

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



Rengeteg api fut.





b,c:Nem tudom, akár hogy próbáltam értelmezni, nincs meg a szükséges előzetes informatikai tudásom ahhoz, hogy az épp működő folyamatokat értelmezni tudjam.