Operációs rendszerek Bsc

3. gyak.

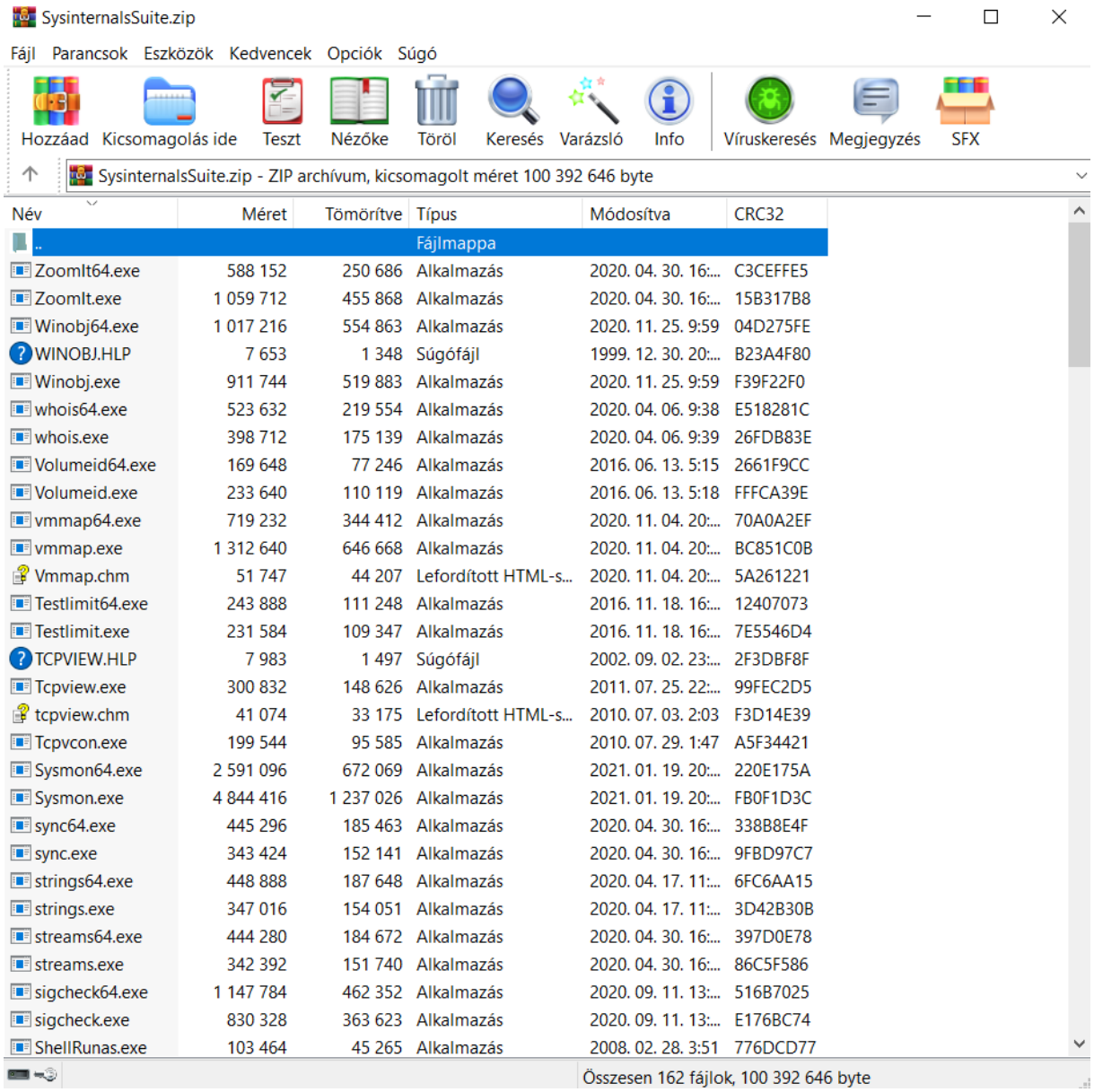
2021. 02. 24.

Készítette:

Takács Bálint Bsc
Programtervező
informatikus
P2GNFT

Miskolc, 2021

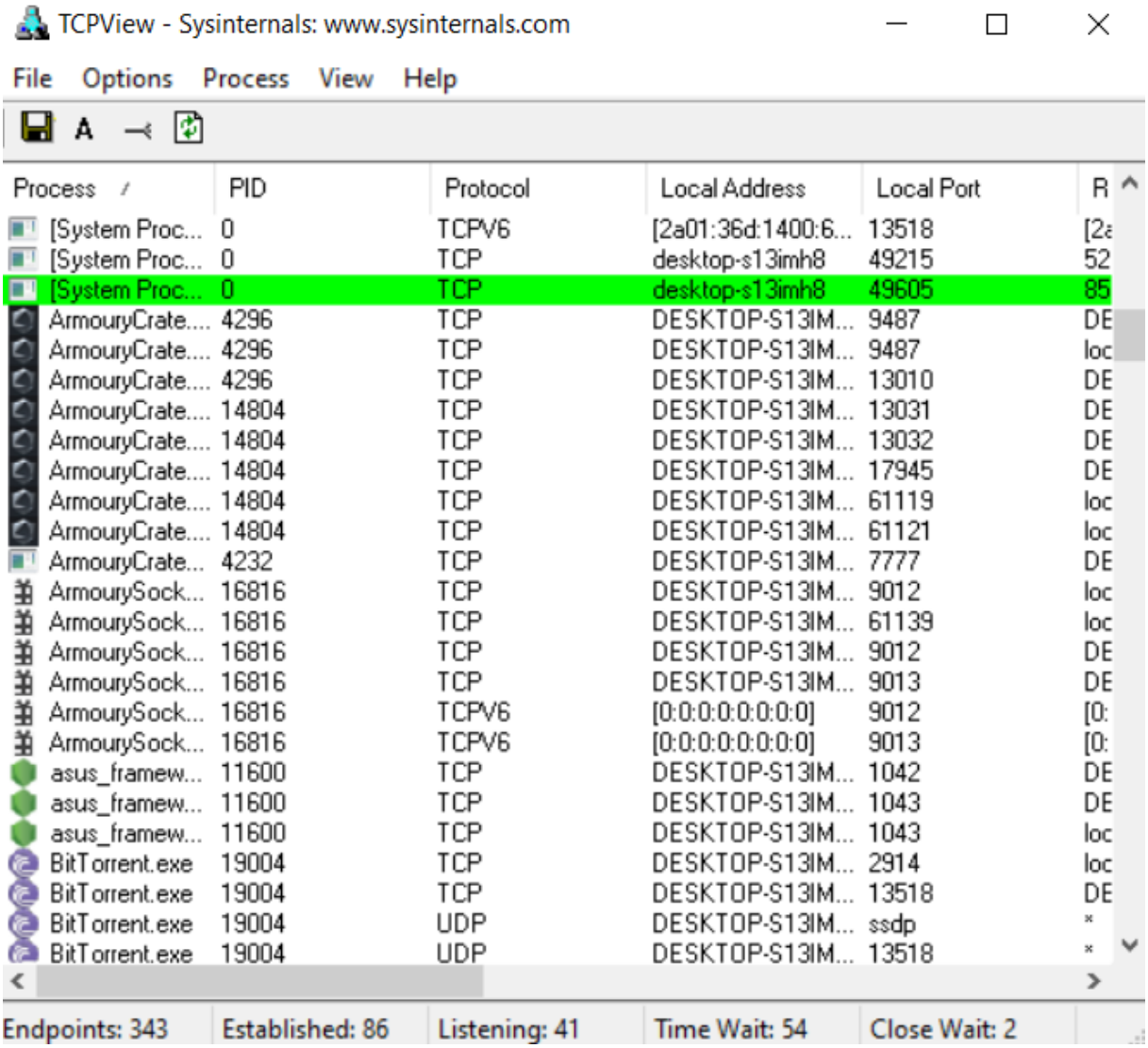
1. **feladat** - Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.
https://docs.microsoft.com/hu-hu/sysinternals/downloads/sysinternals-suite



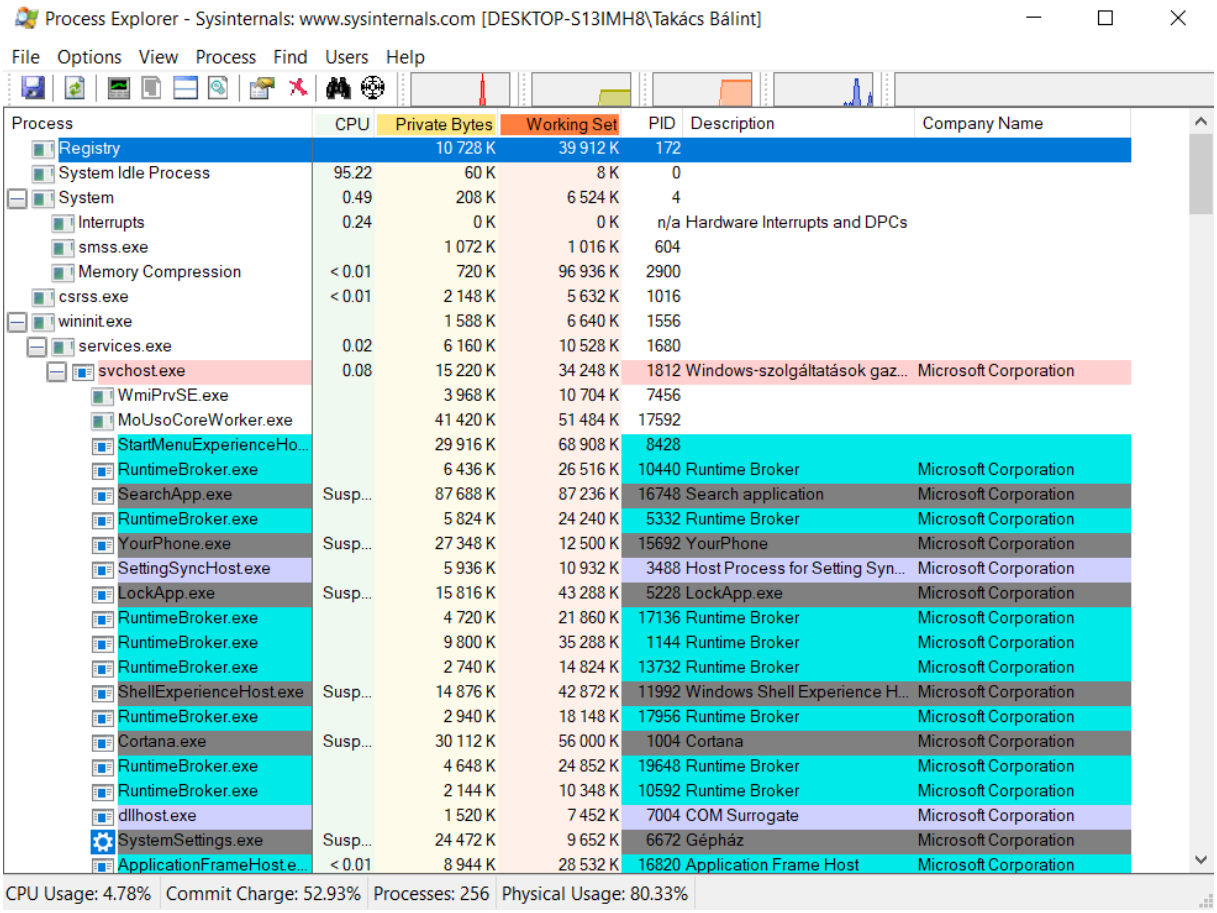
Név	Méret	Tömörítve	Típus	Módosítva	CRC32
..			Fájlmappa		
ZoomIt64.exe	588 152	250 686	Alkalmazás	2020. 04. 30. 16:...	C3CEFFE5
ZoomIt.exe	1 059 712	455 868	Alkalmazás	2020. 04. 30. 16:...	15B317B8
Winobj64.exe	1 017 216	554 863	Alkalmazás	2020. 11. 25. 9:59	04D275FE
WINOBJ.HLP	7 653	1 348	Súgófájl	1999. 12. 30. 20:...	B23A4F80
Winobj.exe	911 744	519 883	Alkalmazás	2020. 11. 25. 9:59	F39F22F0
whois64.exe	523 632	219 554	Alkalmazás	2020. 04. 06. 9:38	E518281C
whois.exe	398 712	175 139	Alkalmazás	2020. 04. 06. 9:39	26FDB83E
Volumeid64.exe	169 648	77 246	Alkalmazás	2016. 06. 13. 5:15	2661F9CC
Volumeid.exe	233 640	110 119	Alkalmazás	2016. 06. 13. 5:18	FFFCA39E
vmmap64.exe	719 232	344 412	Alkalmazás	2020. 11. 04. 20:...	70A0A2EF
vmmap.exe	1 312 640	646 668	Alkalmazás	2020. 11. 04. 20:...	BC851C0B
Vmmap.chm	51 747	44 207	Lefordított HTML-s...	2020. 11. 04. 20:...	5A261221
Testlimit64.exe	243 888	111 248	Alkalmazás	2016. 11. 18. 16:...	12407073
Testlimit.exe	231 584	109 347	Alkalmazás	2016. 11. 18. 16:...	7E5546D4
TCPVIEW.HLP	7 983	1 497	Súgófájl	2002. 09. 02. 23:...	2F3DBF8F
Tcpview.exe	300 832	148 626	Alkalmazás	2011. 07. 25. 22:...	99FEC2D5
tcpview.chm	41 074	33 175	Lefordított HTML-s...	2010. 07. 03. 2:03	F3D14E39
Tcpvcon.exe	199 544	95 585	Alkalmazás	2010. 07. 29. 1:47	A5F34421
Sysmon64.exe	2 591 096	672 069	Alkalmazás	2021. 01. 19. 20:...	220E175A
Sysmon.exe	4 844 416	1 237 026	Alkalmazás	2021. 01. 19. 20:...	FB0F1D3C
sync64.exe	445 296	185 463	Alkalmazás	2020. 04. 30. 16:...	338B8E4F
sync.exe	343 424	152 141	Alkalmazás	2020. 04. 30. 16:...	9FBD97C7
strings64.exe	448 888	187 648	Alkalmazás	2020. 04. 17. 11:...	6FC6AA15
strings.exe	347 016	154 051	Alkalmazás	2020. 04. 17. 11:...	3D42B30B
streams64.exe	444 280	184 672	Alkalmazás	2020. 04. 30. 16:...	397D0E78
streams.exe	342 392	151 740	Alkalmazás	2020. 04. 30. 16:...	86C5F586
sigcheck64.exe	1 147 784	462 352	Alkalmazás	2020. 09. 11. 13:...	516B7025
sigcheck.exe	830 328	363 623	Alkalmazás	2020. 09. 11. 13:...	E176BC74
ShellRunas.exe	103 464	45 265	Alkalmazás	2008. 02. 28. 3:51	776DCD77

Összesen 162 fájlok, 100 392 646 byte

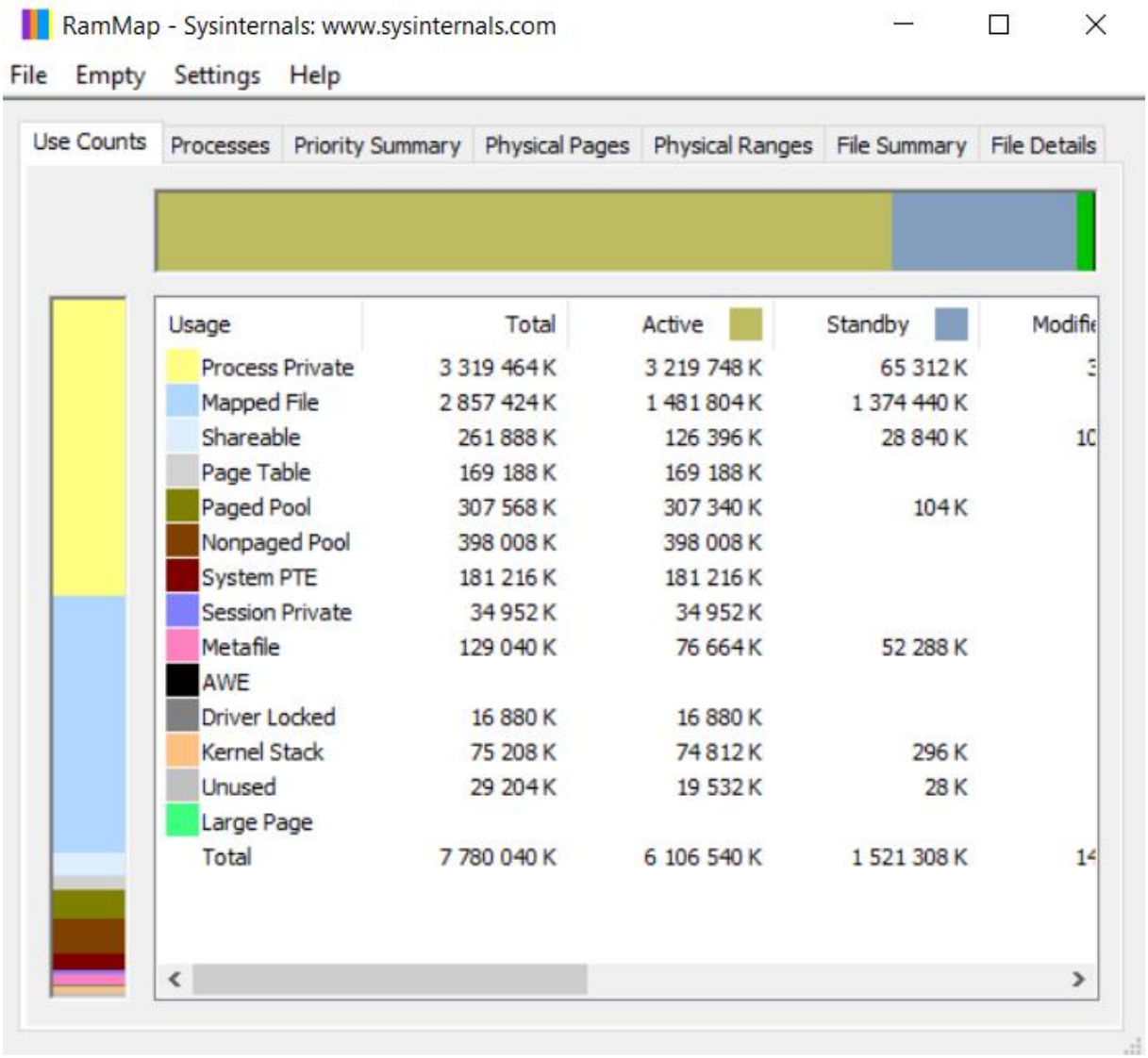
2. **feladat** - A felsorolt eszközök közül minden eszköz esetén töltse le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét egy-egy mondattal - majd mentse el a megadott dokumentumba (képernyőkép).



A TCP View segédprogramon keresztül a laptopomon jelenleg futó hálózati aktivitásokat láthatom.

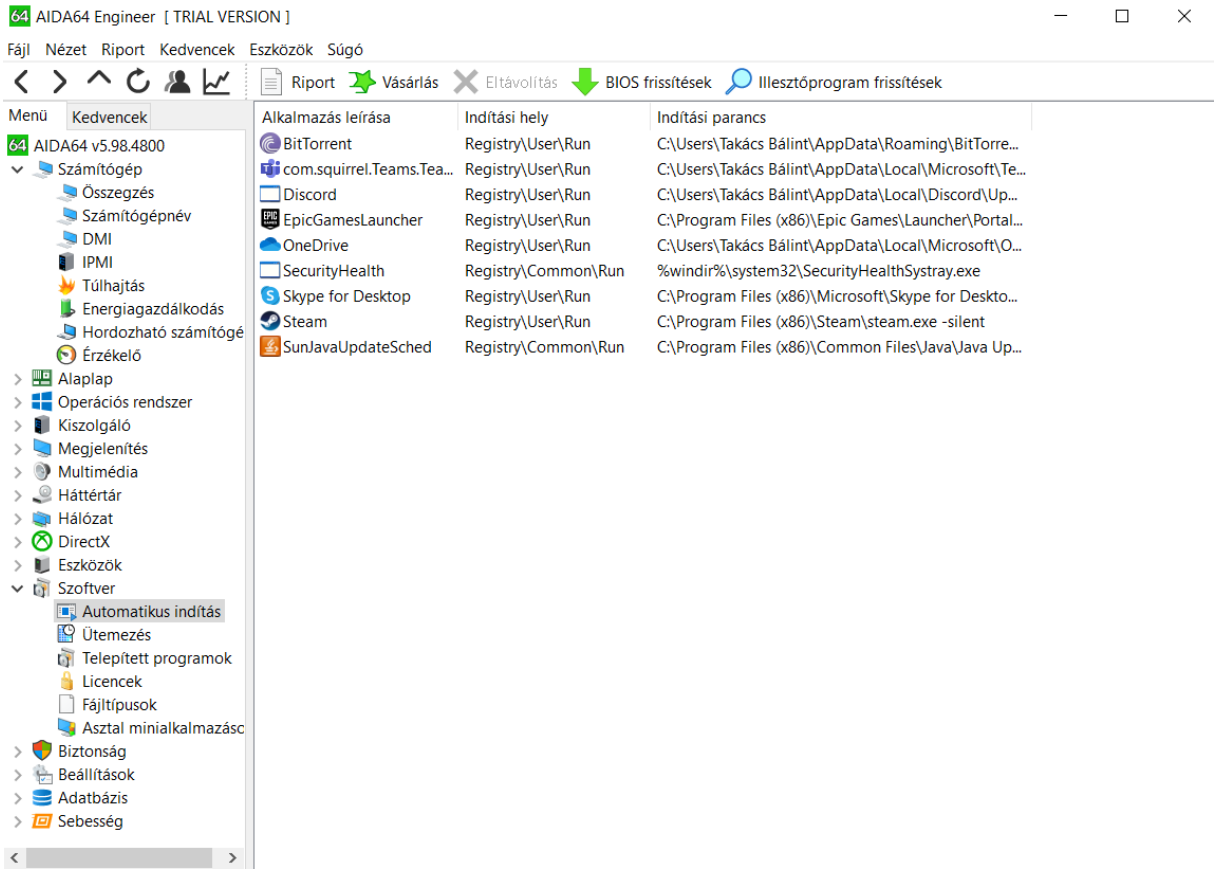


A Process Explorer lényegében egy komplexebb feladatkezelő mint a Windows alapértelmezett feladatkezelője. Ebben a programban az láthatjuk , hogy milyen műveletek futnak jelenleg a számítógépen.



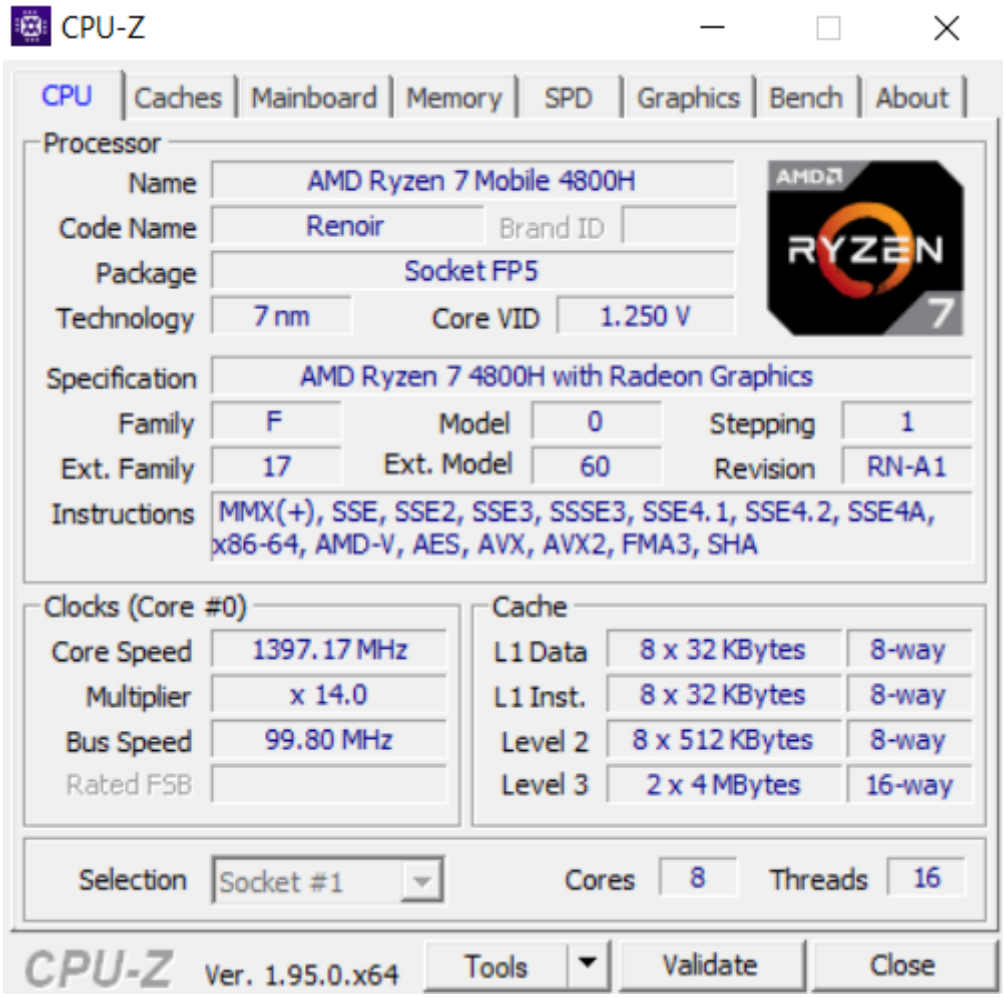
A RAM Map -ban a számítógépben megtalálható memória felhasználásának eloszlását vizsgálhatjuk.

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

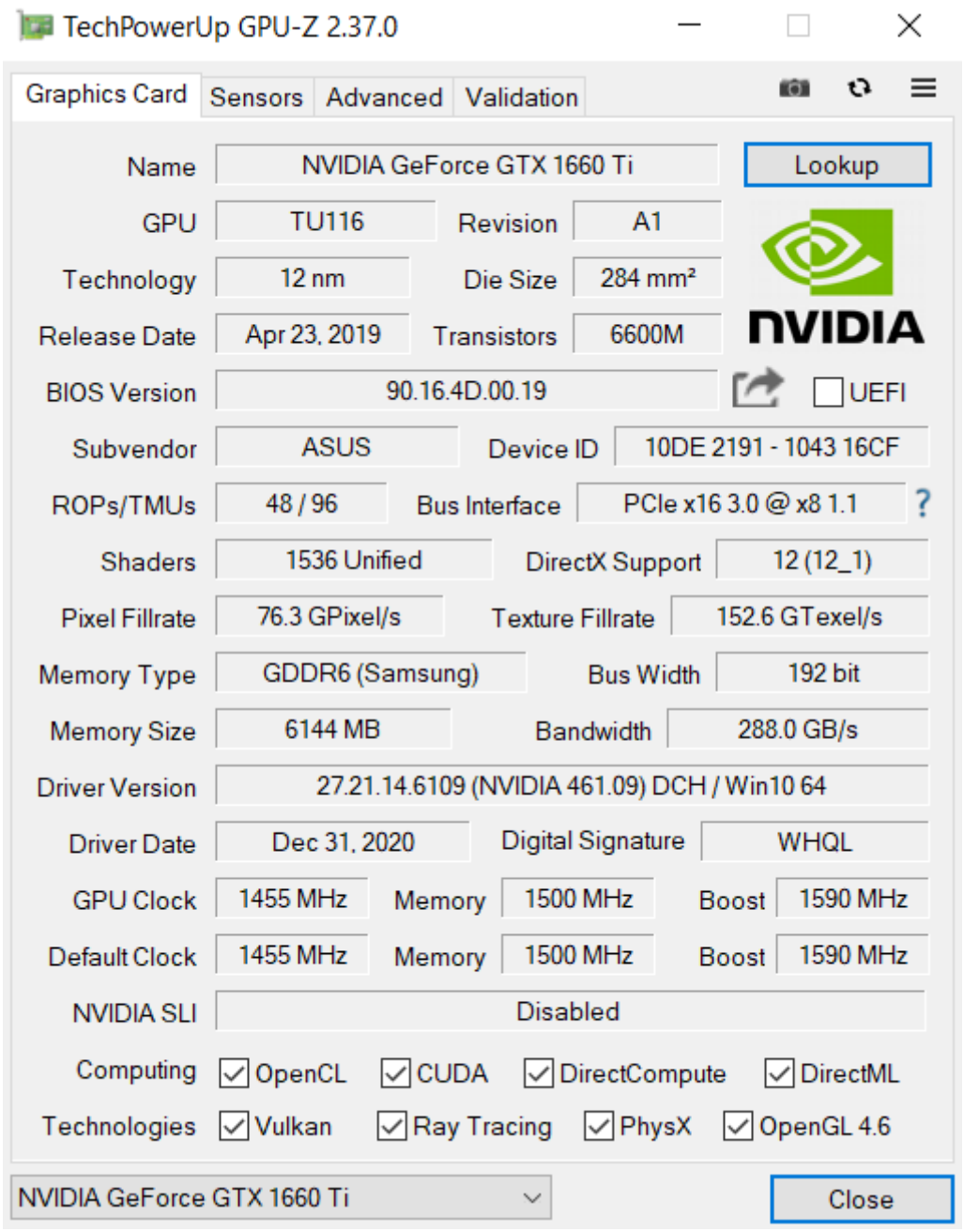

AIDA64 Engineer [TRIAL VERSION]
Fájl Nézet Riport Kedvencek Eszközök Súgó
Riport Vásárlás Eltávolítás BIOS frissítések Illesztőprogram frissítések
Menü Kedvencek
AIDA64 v5.98.4800
Számítógép
Összegzés
Számítógépnév
DMI
IPMI
Túlhajtás
Energiagazdálkodás
Hordozható számítógé
Érzékelő
Alaplap
Operációs rendszer
Kiszolgáló
Megjelenítés
Multimédia
Háttértár
Hálózat
DirectX
Eszközök
Szoftver
Automatikus indítás
Ütemezés
Telepített programok
Licencek
Fájltípusok
Asztal minialkalmazásc
Biztonság
Beállítások
Adatbázis
Sebesség
Alkalmazás leírása
Indítási hely
Indítási parancs
BitTorrent
Registry\User\Run
C:\Users\Takács Bálint\AppData\Roaming\BitTorre...
com.squirrel.Teams.Tea...
Registry\User\Run
C:\Users\Takács Bálint\AppData\Local\Microsoft\Te...
Discord
Registry\User\Run
C:\Users\Takács Bálint\AppData\Local\Discord\Up...
EpicGamesLauncher
Registry\User\Run
C:\Program Files (x86)\Epic Games\Launcher\Portal...
OneDrive
Registry\User\Run
C:\Users\Takács Bálint\AppData\Local\Microsoft\O...
SecurityHealth
Registry\Common\Run
%windir%\system32\SecurityHealthSystray.exe
Skype for Desktop
Registry\User\Run
C:\Program Files (x86)\Microsoft\Skype for Deskto...
Steam
Registry\User\Run
C:\Program Files (x86)\Steam\steam.exe -silent
SunJavaUpdateSched
Registry\Common\Run
C:\Program Files (x86)\Common Files\Java\Java Up...

Az AIDA64 Engineer – rel hardver szoftver és operációs diagnosztikát hajthatunk végre a számítógépünkön , de ezek mellett még rengetek műveletet hajthatunk végre vele pl.: hibakeresést, érzékelőfigyelés, sebességmérés stb.

Az első fenti képen azt vizsgáltam , hogy milyen programok indulnak automatikusan a rendszer indulásával együtt.
A másodikon pedig egy GPGPU Benchmark eredményei láthatóak.



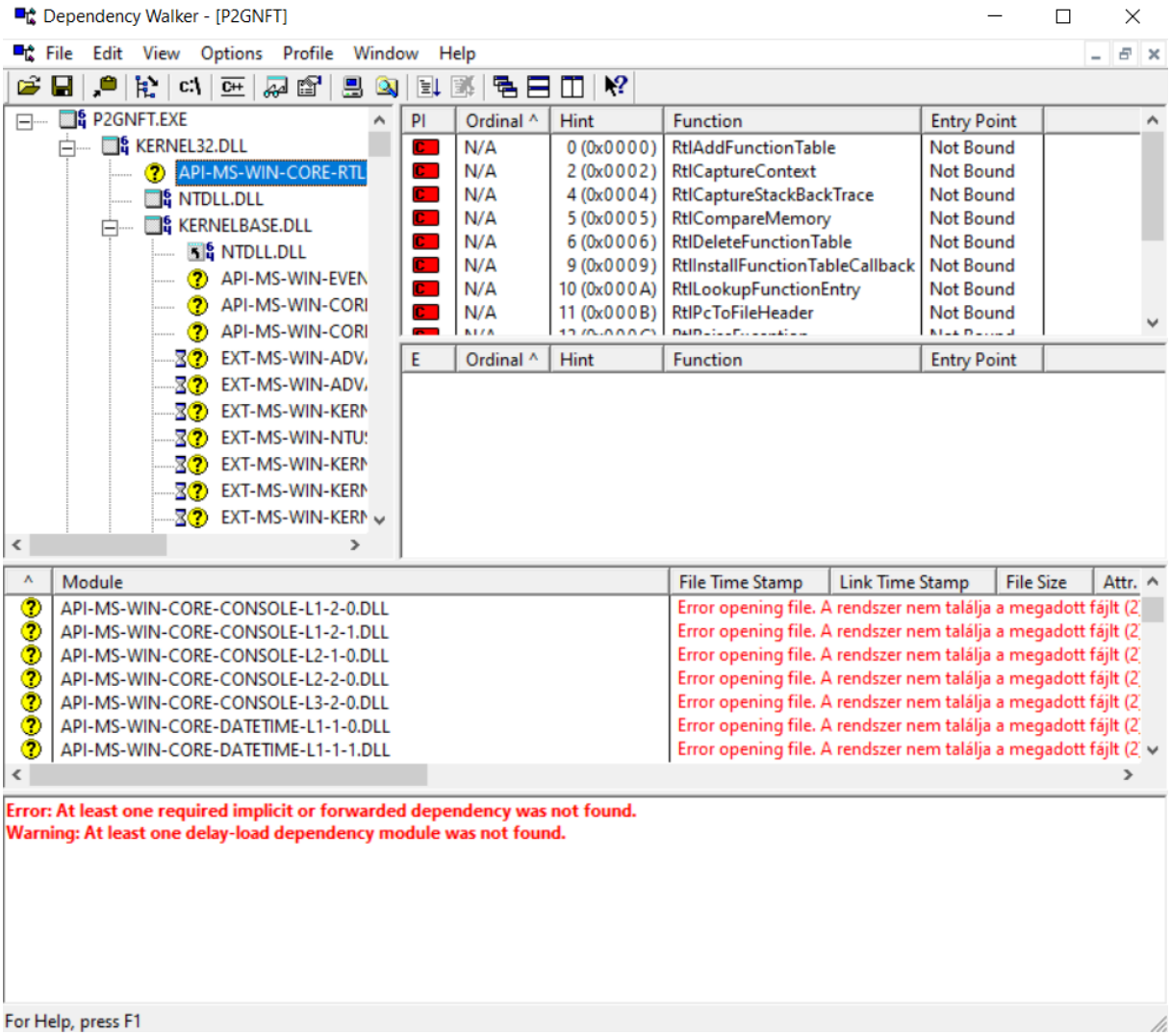
A CPU-Z program a processzoromról gyűjt ki adatokat.

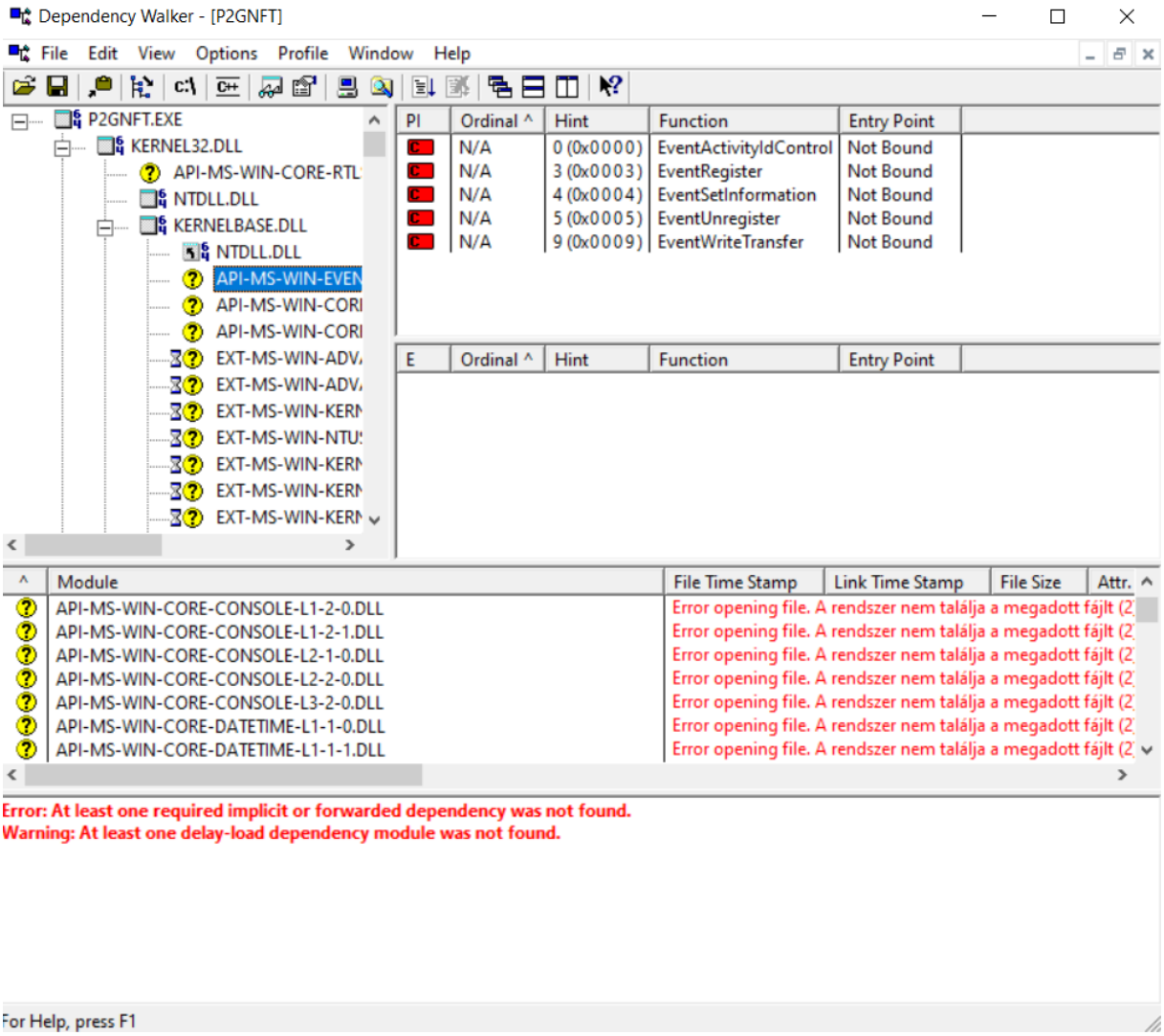


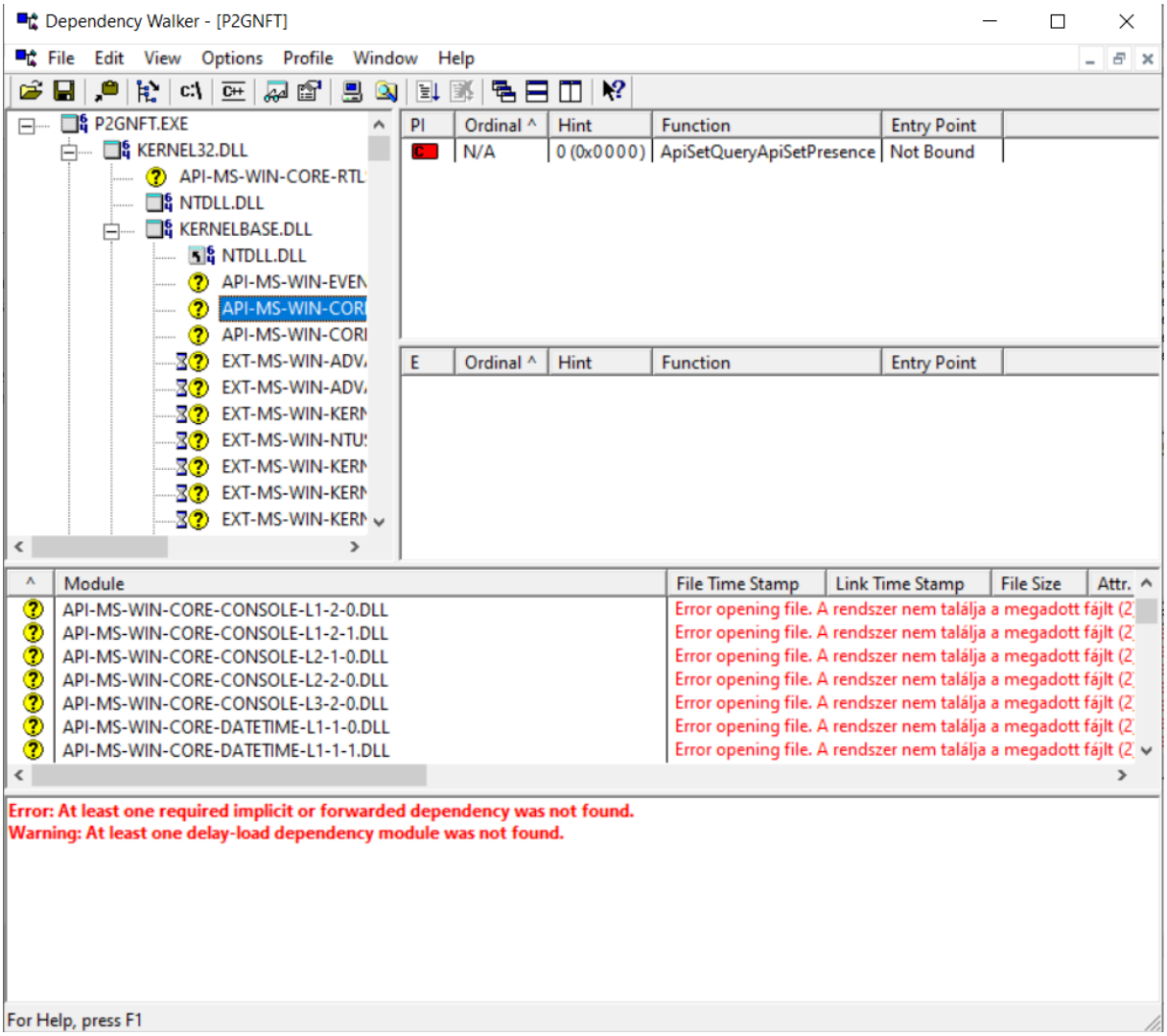
A GPU-Z program a számítógépemben megtalálható grafikus meghajtóról vagyis a videókártyáról gyűjt ki adatokat.

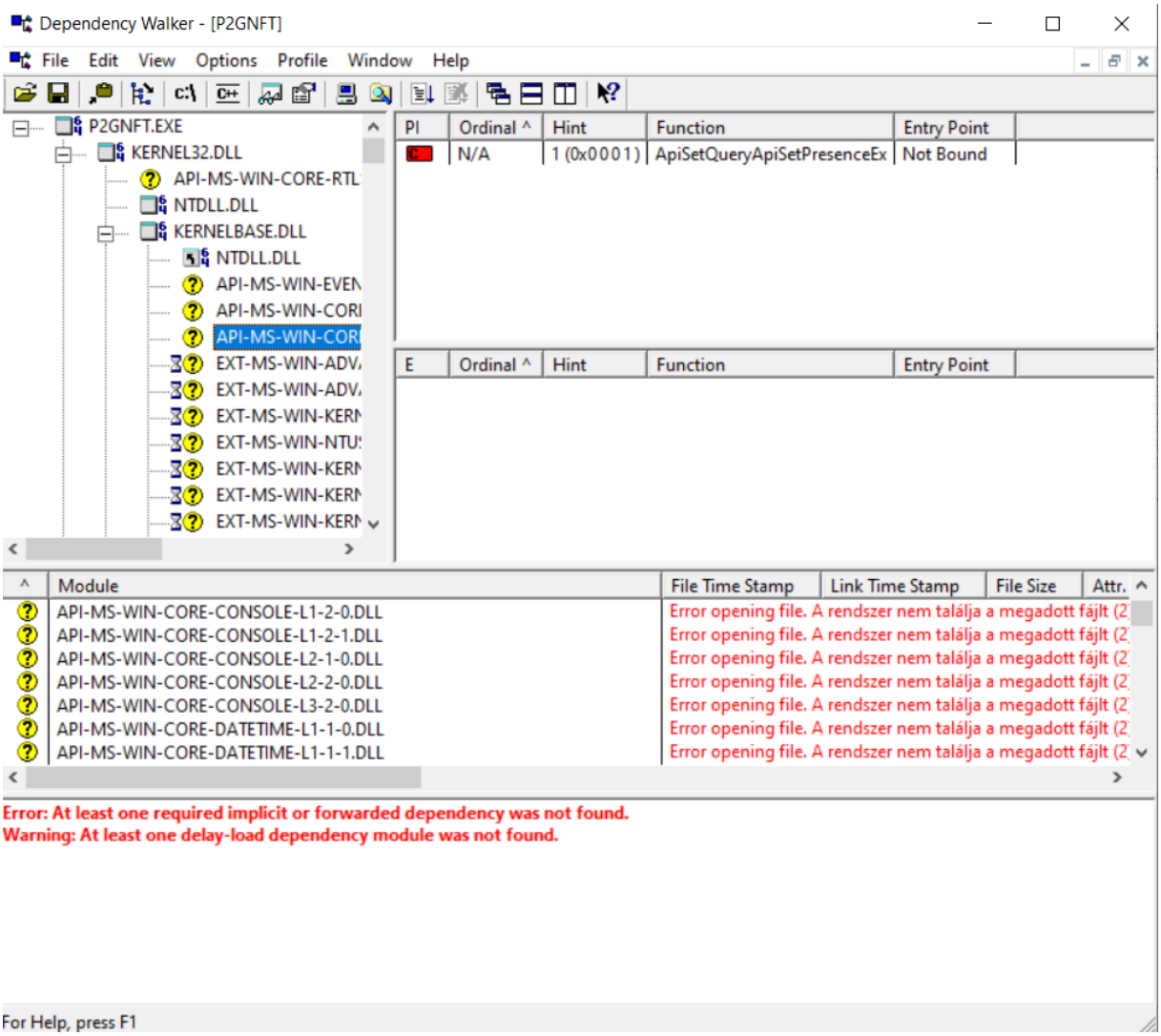
4. **feladat -** A Dependency Walker segítségével végezze el a következő feladatokat.

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


Dependency Walker - [P2GNFT]
File Edit View Options Profile Window Help
P2GNFT.EXE
KERNEL32.DLL
API-MS-WIN-CORE-RTL
NTDLL.DLL
KERNELBASE.DLL
NTDLL.DLL
API-MS-WIN-EVEN
API-MS-WIN-CORI
API-MS-WIN-CORI
EXT-MS-WIN-ADV
EXT-MS-WIN-ADV
EXT-MS-WIN-KERN
EXT-MS-WIN-NTU
EXT-MS-WIN-KERN
EXT-MS-WIN-KERN
EXT-MS-WIN-KERN
PI Ordinal ^ Hint Function Entry Point
N/A 0 (0x0000) RtlAddFunctionTable Not Bound
N/A 2 (0x0002) RtlCaptureContext Not Bound
N/A 4 (0x0004) RtlCaptureStackBackTrace Not Bound
N/A 5 (0x0005) RtlCompareMemory Not Bound
N/A 6 (0x0006) RtlDeleteFunctionTable Not Bound
N/A 9 (0x0009) RtlInstallFunctionTableCallback Not Bound
N/A 10 (0x000A) RtlLookupFunctionEntry Not Bound
N/A 11 (0x000B) RtlPcToFileHeader Not Bound
E Ordinal ^ Hint Function Entry Point
^ Module File Time Stamp Link Time Stamp File Size Attr.
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-DATETIME-L1-1-1.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.
For Help, press F1


Dependency Walker - [P2GNFT]
File Edit View Options Profile Window Help
P2GNFT.EXE
KERNEL32.DLL
API-MS-WIN-CORE-RTL
NTDLL.DLL
KERNELBASE.DLL
NTDLL.DLL
API-MS-WIN-EVEN
API-MS-WIN-CORI
API-MS-WIN-CORI
EXT-MS-WIN-ADV
EXT-MS-WIN-ADV
EXT-MS-WIN-KERN
EXT-MS-WIN-NTU
EXT-MS-WIN-KERN
EXT-MS-WIN-KERN
EXT-MS-WIN-KERN
PI Ordinal ^ Hint Function Entry Point
N/A 0 (0x0000) EventActivityIdControl Not Bound
N/A 3 (0x0003) EventRegister Not Bound
N/A 4 (0x0004) EventSetInformation Not Bound
N/A 5 (0x0005) EventUnregister Not Bound
N/A 9 (0x0009) EventWriteTransfer Not Bound
E Ordinal ^ Hint Function Entry Point
Module File Time Stamp Link Time Stamp File Size Attr.
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL
API-MS-WIN-CORE-DATETIME-L1-1-1.DLL
Error opening file. A rendszer nem találja a megadott fájlt (2
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.
For Help, press F1


Dependency Walker - [P2GNFT]
File Edit View Options Profile Window Help
P2GNFT.EXE
KERNEL32.DLL
API-MS-WIN-CORE-RTL
NTDLL.DLL
KERNELBASE.DLL
NTDLL.DLL
API-MS-WIN-EVEN
API-MS-WIN-COR
API-MS-WIN-CORI
EXT-MS-WIN-ADV
EXT-MS-WIN-ADV
EXT-MS-WIN-KERN
EXT-MS-WIN-NTU
EXT-MS-WIN-KERN
EXT-MS-WIN-KERN
EXT-MS-WIN-KERN
PI Ordinal ^ Hint Function Entry Point
N/A 0 (0x0000) ApiSetQueryApiSetPresence Not Bound
E Ordinal ^ Hint Function Entry Point
Module File Time Stamp Link Time Stamp File Size Attr.
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL
API-MS-WIN-CORE-DATETIME-L1-1-1.DLL
Error opening file. A rendszer nem találja a megadott fájlt (2
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.
For Help, press F1


Dependency Walker - [P2GNFT]
File Edit View Options Profile Window Help
P2GNFT.EXE
KERNEL32.DLL
API-MS-WIN-CORE-RTL
NTDLL.DLL
KERNELBASE.DLL
NTDLL.DLL
API-MS-WIN-EVEN
API-MS-WIN-CORI
API-MS-WIN-COR
EXT-MS-WIN-ADV
EXT-MS-WIN-ADV
EXT-MS-WIN-KERN
EXT-MS-WIN-NTU
EXT-MS-WIN-KERN
EXT-MS-WIN-KERN
EXT-MS-WIN-KERN
PI Ordinal ^ Hint Function Entry Point
C N/A 1 (0x0001) ApiSetQueryApiSetPresenceEx Not Bound
E Ordinal ^ Hint Function Entry Point
Module File Time Stamp Link Time Stamp File Size Attr.
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
API-MS-WIN-CORE-DATETIME-L1-1-1.DLL Error opening file. A rendszer nem találja a megadott fájlt (2
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.
For Help, press F1

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