

Operációs rendszerek BSc

3.gyak.

2021. 02. 24.

Készítette:

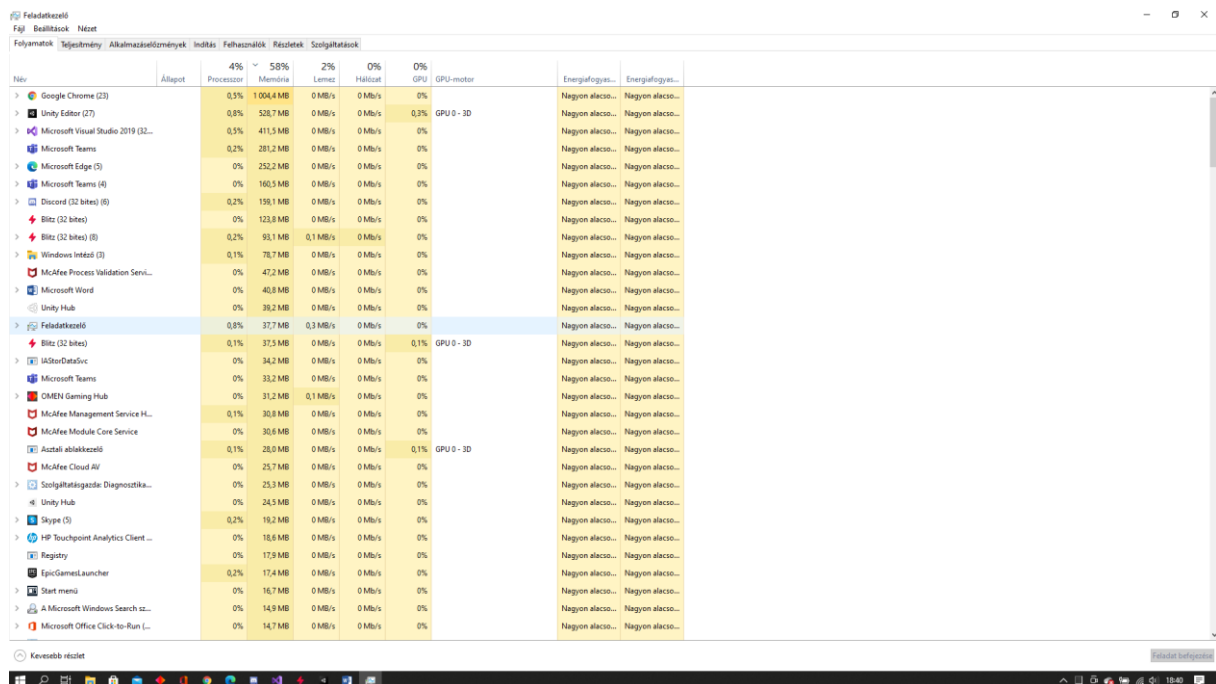
Palkó Patrik Dávid Bsc

Programtervező Informatikus szak

ZW7DOR

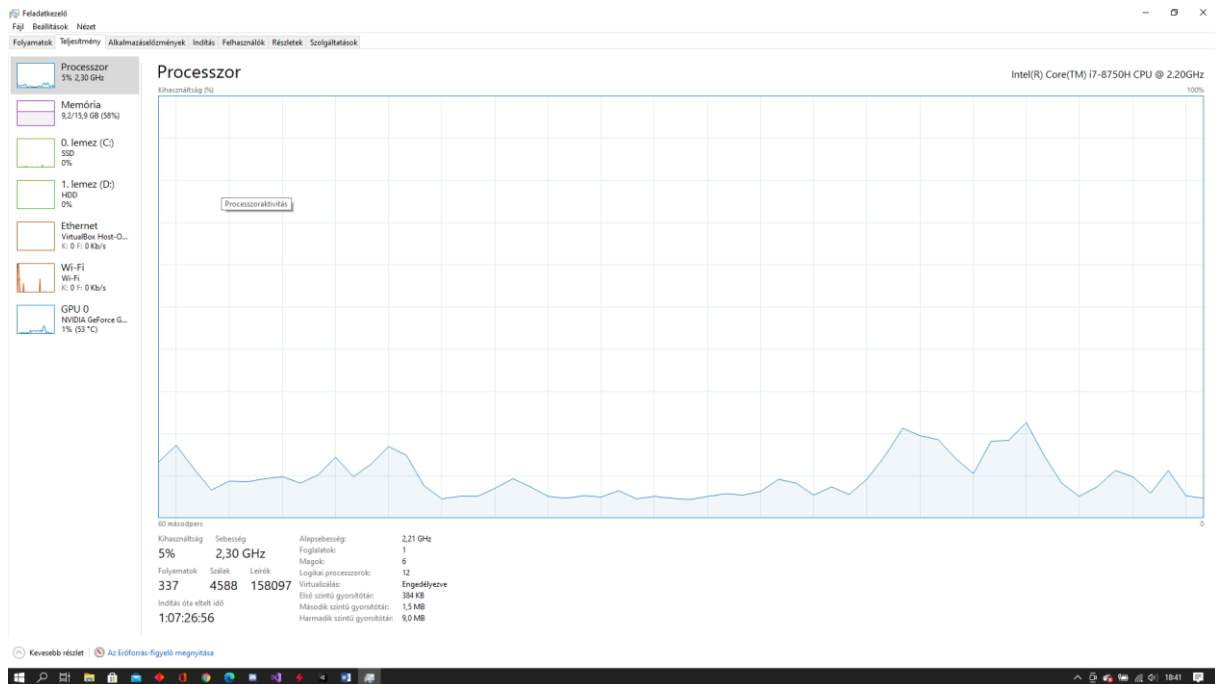
Miskolc, 2021

1.feladat A Windows belső működésének a tanulmányozása.



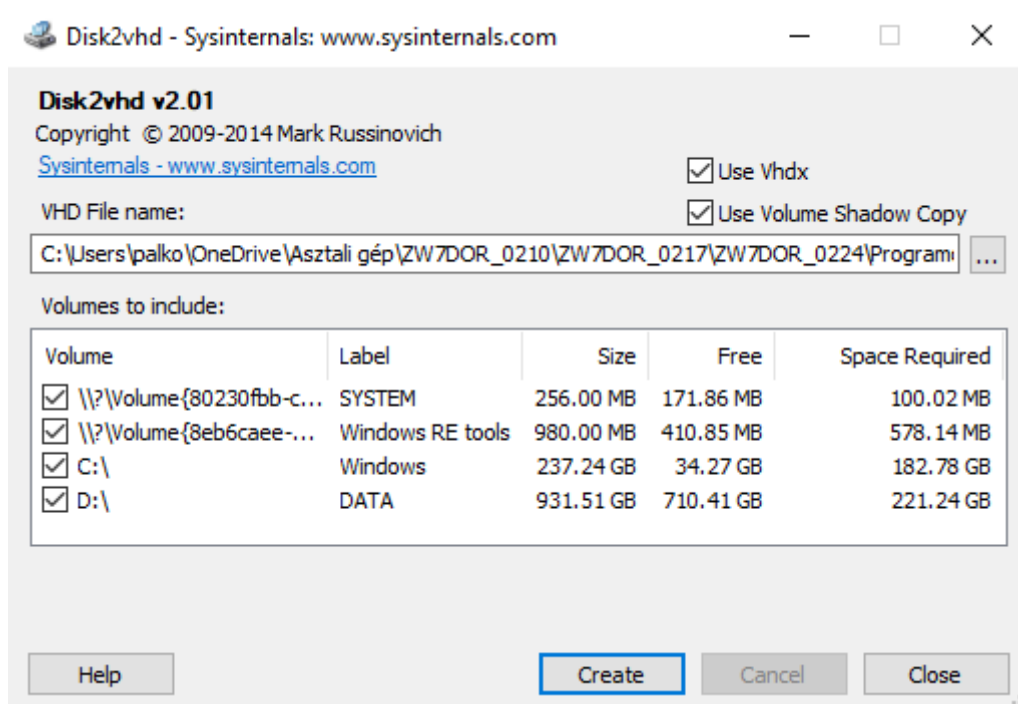
The screenshot shows the Windows Task Manager Performance tab. The top bar indicates system status: Fáj, Beállítások, Nézet. Below the tabs, a summary bar shows: Folyamatok, Teljesítmény, Alkalmazásüzemeltetés, Indítás, Felhasználók, Részletek, Szolgáltatások. The main area displays a table of system resources with columns: Név, Állapot, 4%, 58%, 2%, 0%, 0%, GPU, GPU-motor, Energiafelhasználás, and Energiafelhasználás. The table lists various system components and their current usage percentages and memory usage.

Név	Állapot	4%	58%	2%	0%	0%	GPU	GPU-motor	Energiafelhasználás	Energiafelhasználás
Google Chrome (22)		0,3%	1 004,4 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Unity Editor (27)		0,6%	528,7 MB	0 MB/s	0 MB/s	0,3%	GPU 0 - 3D		Nagyon alacsony	Nagyon alacsony
Microsoft Visual Studio 2019 (32...)		0,5%	411,5 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Microsoft Teams		0,2%	281,2 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Microsoft Edge (5)		0%	252,2 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Microsoft Teams (4)		0%	160,5 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Discord (32 bites) (6)		0,2%	158,1 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Blitz (32 bites) (8)		0%	123,8 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Blitz (32 bites) (8)		0,2%	93,1 MB	0,1 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Windows Indent (3)		0,1%	78,7 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
McAfee Process Validation Servi...		0%	47,2 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Microsoft Word		0%	40,8 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Unity Hub		0%	39,2 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Feladatkezelő		0,8%	37,7 MB	0,3 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Blitz (32 bites)		0,1%	37,5 MB	0 MB/s	0 MB/s	0,1%	GPU 0 - 3D		Nagyon alacsony	Nagyon alacsony
IAStarDetective		0%	34,2 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Microsoft Teams		0%	33,2 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
OMEN Gaming Hub		0%	31,2 MB	0,1 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
McAfee Management Service H...		0,1%	30,8 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
McAfee Module Core Service		0%	30,6 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Acrobat alkalmazás		0,1%	28,0 MB	0 MB/s	0 MB/s	0,1%	GPU 0 - 3D		Nagyon alacsony	Nagyon alacsony
McAfee Cloud AI		0%	25,7 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Szolgáltatáskezelő: Diagnosztika...		0%	25,3 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Unity Hub		0%	24,5 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Skype (5)		0,2%	19,2 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
HP Touchpoint Analytics Client ...		0%	18,6 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Registry		0%	17,9 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
EpicGamesLauncher		0,2%	17,4 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Start menü		0%	16,7 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
A Microsoft Windows Search sz...		0%	14,9 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony
Microsoft Office Click-to-Run L...		0%	14,7 MB	0 MB/s	0 MB/s	0%			Nagyon alacsony	Nagyon alacsony



2.Feladat A Sysinternals Suite programcsomag tanulmányozása.

a, File and Disk Utilities(Disk2vhd)



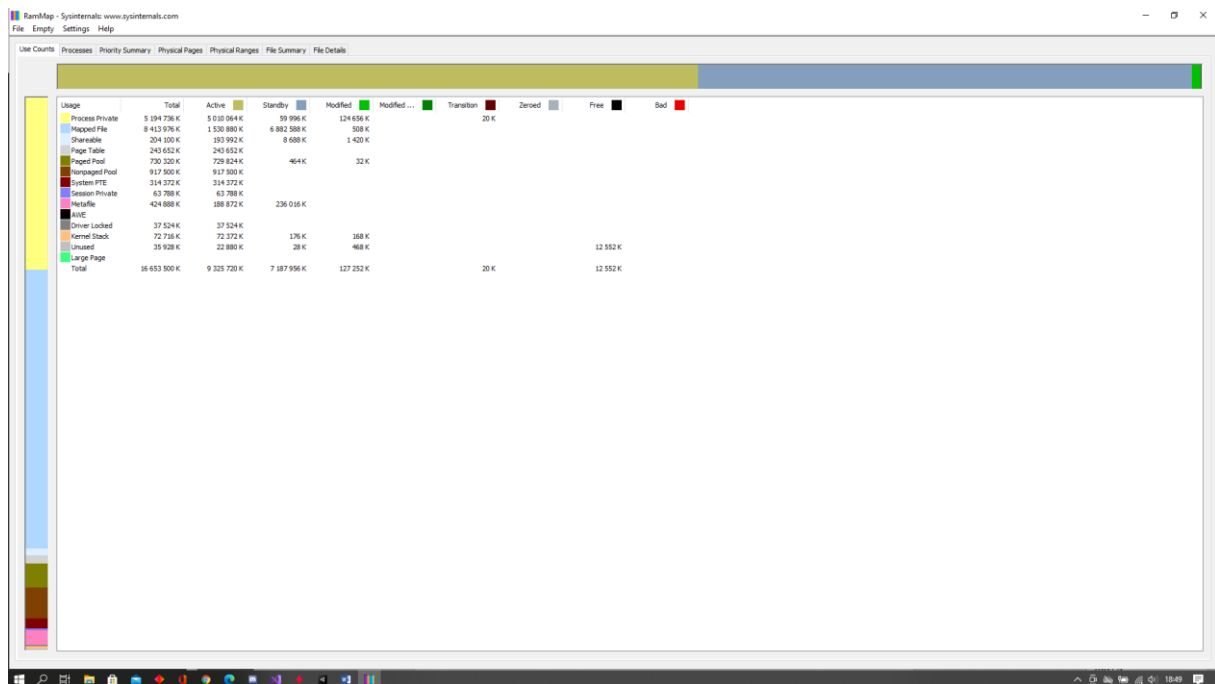
b, Networking Utilities(TCPView)

Process Explorer - SystemInfo: www.systeminfo.com [LAPTOP-BVYM10DF-galle]

File Options View Process Find Help Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	0.00	0 K	0 K	0		
System	0.26	212 K	808 K	4		
smss.exe	0.04	0 K	0 K	8	Hardware Interrupts and DPCs	
svchost.exe	1.040 K	288 K	544			
csrss.exe	2.482 K	775 383 K	3308			
smss.exe	2.012 K	2 860 K	886			
svchost.exe	1.392 K	2 260 K	948			
csrss.exe	6.376 K	8 320 K	1616			
services.exe	16.112 K	23 540 K	1 086	Windows-svcinstallat...	Microsoft Corporation	
Winlogon.exe	14.656 K	20 200 K	3716			
csrss.exe	2.812 K	5 220 K	3038			
Winlogon.exe	5.028 K	9 728 K	2660			
csrss.exe	53.024 K	50 736 K	9020			
RuntimeBroker.exe	6.372 K	17 152 K	10 686	Runtime Broker	Microsoft Corporation	
SearchApp.exe	Sup.	176 716 K	198 188 K	10 672	Search application	Microsoft Corporation
RuntimeBroker.exe	Sup.	21 268 K	41 184 K	10 716	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	Sup.	42 584 K	1 644 K	10 726	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe	11.544 K	5 856 K	11 556	Host Process for Setting Syn...	Microsoft Corporation	
RuntimeBroker.exe	7.460 K	17 216 K	11 602	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe	4.584 K	9 804 K	14 176	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe	Sup.	37 512 K	40 596 K	10 684	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe	Sup.	2 636 K	12 764 K	11 636	Runtime Broker	Microsoft Corporation
SearchIndexingHost.exe	Sup.	36 120 K	15 172 K	20 304		Microsoft Corporation
ApplicationFrameHost.exe	Sup.	38 676 K	26 336 K	20 452	Application Frame Host	Microsoft Corporation
WindowsAppCore.exe	Sup.	75 416 K	4 520 K	20 496		Microsoft Corporation
RuntimeBroker.exe	6.112 K	6 496 K	19 440	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe	Sup.	46 080 K	1 528 K	19 468	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	Sup.	39 304 K	30 472 K	13 034		Microsoft Corporation
RuntimeBroker.exe	Sup.	2 268 K	5 164 K	18 880	User Score Broker	Microsoft Corporation
csrss.exe	4.656 K	12 532 K	14 020	COM Surrogate	Microsoft Corporation	
FileCache.exe	5.532 K	8 892 K	40 712	Microsoft OneDriveFile Co...	Microsoft Corporation	
RuntimeBroker.exe	Sup.	83 040 K	2 084 K	18 888		Microsoft Corporation
RuntimeBroker.exe	Sup.	10 816 K	24 492 K	14 032	Runtime Broker	Microsoft Corporation
csrss.exe	3.656 K	6 060 K	11 572			
ComponentHost.exe	2.652 K	5 788 K	18 804	Component Package Support	Microsoft Corporation	
LinkApp.exe	Sup.	36 300 K	42 164 K	20 712	LinkApp.exe	Microsoft Corporation
RuntimeBroker.exe	Sup.	10 028 K	35 344 K	21 020	Runtime Broker	Microsoft Corporation
CalcHost.exe	Sup.	44 332 K	5 700 K	19 972		Microsoft Corporation
RuntimeBroker.exe	Sup.	1 320 K	6 560 K	20 668	Runtime Broker	Microsoft Corporation
csrss.exe	2.960 K	13 512 K	20 628			
malware.exe	8.312 K	23 576 K	14 432	Windows Defender SmartSc...	Microsoft Corporation	
SearchApp.exe	<0.01	100 608 K	159 228 K	10 678	Search application	Microsoft Corporation
WUTrusted.exe	0.916 K	6.832 K	10 55			
csrss.exe	<0.01	11 800 K	15 572 K	10 888	Windows-svcinstallat...	Microsoft Corporation
csrss.exe	3.240 K	5 320 K	11 584	Windows-svcinstallat...	Microsoft Corporation	
csrss.exe	1.880 K	3 004 K	14 776	Windows-svcinstallat...	Microsoft Corporation	
csrss.exe	3.196 K	6 796 K	14 848	Windows-svcinstallat...	Microsoft Corporation	
csrss.exe	1.884 K	4 728 K	14 852	Windows-svcinstallat...	Microsoft Corporation	
csrss.exe	2.600 K	6 076 K	15 228	Windows-svcinstallat...	Microsoft Corporation	
csrss.exe	1.932 K	4 384 K	15 336	Windows-svcinstallat...	Microsoft Corporation	
csrss.exe	6.720 K	10 488 K	17 036	Windows-svcinstallat...	Microsoft Corporation	
csrss.exe	3.632 K	992 K	896			
csrss.exe	11 660 K	15 764 K	8240	Catalyst Windows Fea...	Microsoft Corporation	
csrss.exe	35 312 K	13 108 K	124	IFADSwitch	Microsoft Corporation	
csrss.exe	5 764 K	8 184 K	22 968			
csrss.exe	2 180 K	4 644 K	17 796			
csrss.exe	1.988 K	3 060 K	18 12	Windows-svcinstallat...	Microsoft Corporation	

e, Information Utilities(RAMMap)

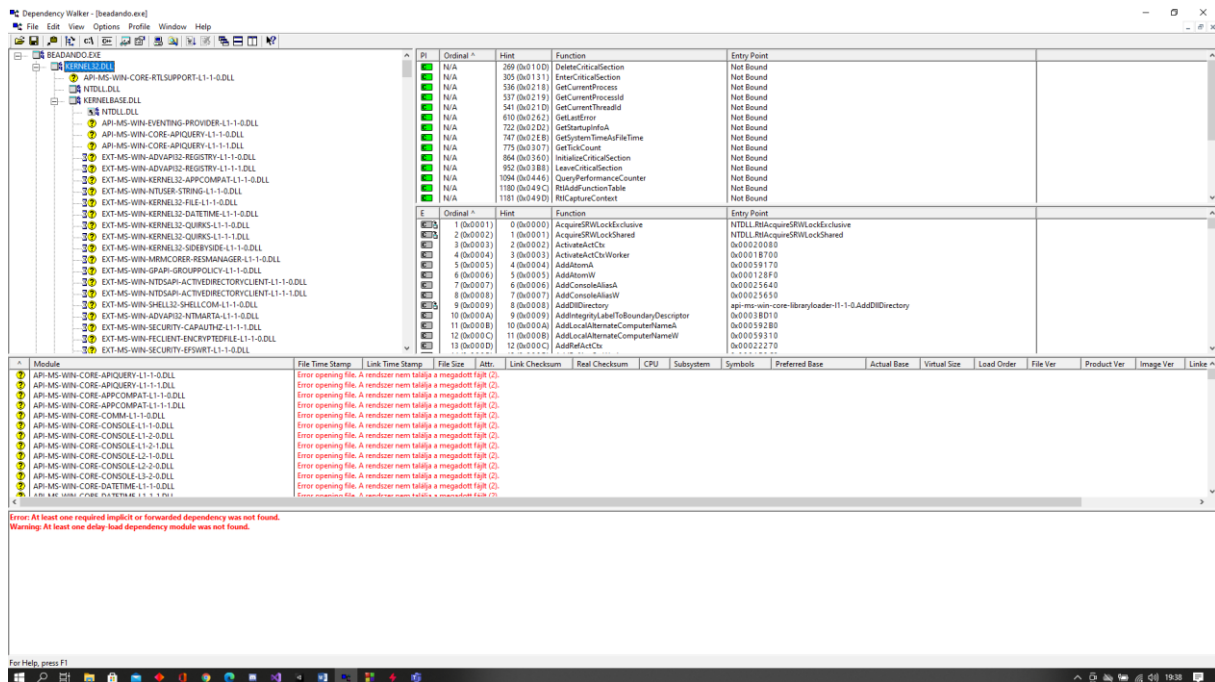


Process	Session	PID	Private	Standby	Modified	Page Table	Total
AutMService...	0	4884	372 K	0 K	0 K	228 K	600 K
System	-1	4	0 K	0 K	0 K	96 K	96 K
Registry	-1	148	19 904 K	12 K	0 K	348 K	20 264 K
svchost.exe	0	4712	1 736 K	0 K	0 K	500 K	2 236 K
smss.exe	-1	544	96 K	0 K	0 K	148 K	244 K
notepad.exe	1	19792	0 K	0 K	0 K	36 K	36 K
chrome.exe	1	14536	0 K	0 K	0 K	44 K	44 K
blitz.exe	1	23288	2 892 K	0 K	0 K	720 K	3 612 K
blitz.exe	1	2636	2 928 K	0 K	0 K	712 K	3 640 K
blitz.exe	1	23292	2 888 K	0 K	0 K	712 K	3 600 K
chrome.exe	1	3564	70 584 K	2 284 K	5 064 K	2 256 K	80 188 K
conhost.exe	1	10040	600 K	0 K	4 K	304 K	908 K
blitz.exe	1	23348	2 868 K	4 K	0 K	724 K	3 596 K
ProdInfo.exe	1	12908	0 K	0 K	0 K	28 K	28 K
blitz.exe	1	23320	2 916 K	16 K	0 K	720 K	3 652 K
smss.exe	0	632	0 K	0 K	0 K	32 K	32 K
notepad.exe	0	4700	9 792 K	12 K	0 K	716 K	10 520 K
LockApp.exe	1	23712	408 K	776 K	0 K	912 K	2 096 K
svchost.exe	0	880	1 036 K	0 K	0 K	344 K	1 380 K
csrss.exe	1	956	1 024 K	0 K	0 K	280 K	1 304 K
csrss.exe	0	856	724 K	0 K	0 K	248 K	972 K
svchost.exe	0	948	20 K	0 K	8 K	232 K	260 K
services.exe	0	1016	4 384 K	0 K	92 K	280 K	4 756 K
lsass.exe	0	356	4 668 K	24 K	0 K	412 K	7 124 K
svchost.exe	0	836	11 140 K	0 K	0 K	572 K	11 712 K
fordsh-vhost.exe	0	604	164 K	0 K	0 K	180 K	344 K
WdCPHost.exe	0	1036	2 364 K	4 K	0 K	304 K	2 676 K
svchost.exe	0	1088	9 940 K	8 K	0 K	400 K	10 348 K
svchost.exe	0	1164	1 872 K	0 K	0 K	280 K	2 152 K
svchost.exe	1	1252	876 K	0 K	0 K	316 K	1 192 K
fordsh-vhost.exe	1	1308	1 740 K	4 K	0 K	296 K	2 040 K
dm.exe	1	1376	28 372 K	200 K	6 016 K	1 128 K	35 716 K
svchost.exe	0	1436	0 K	0 K	0 K	32 K	32 K
svchost.exe	0	1468	0 K	0 K	0 K	36 K	36 K
svchost.exe	0	1476	672 K	0 K	0 K	272 K	944 K
svchost.exe	0	1484	9 488 K	0 K	0 K	316 K	1 004 K
svchost.exe	0	1492	936 K	0 K	0 K	264 K	1 200 K
svchost.exe	0	1628	1 112 K	0 K	0 K	328 K	1 440 K
svchost.exe	0	1636	1 008 K	0 K	0 K	304 K	1 312 K
svchost.exe	0	4828	356 K	0 K	0 K	280 K	636 K
svchost.exe	0	1728	4 466 K	20 K	0 K	360 K	4 876 K
svchost.exe	0	1796	532 K	0 K	0 K	272 K	804 K
svchost.exe	0	1812	488 K	0 K	0 K	264 K	752 K
svchost.exe	0	1804	0 K	0 K	0 K	32 K	32 K
svchost.exe	0	1860	1 160 K	0 K	0 K	432 K	1 592 K
svchost.exe	0	1884	9 352 K	4 K	4 K	312 K	9 672 K
svchost.exe	0	1948	0 K	0 K	0 K	32 K	32 K
svchost.exe	0	2044	1 372 K	0 K	0 K	308 K	1 680 K
UnityShader...	1	23436	1 272 K	0 K	196 K	332 K	1 800 K
svchost.exe	0	1740	832 K	0 K	0 K	356 K	1 188 K
svchost.exe	0	2448	0 K	0 K	0 K	32 K	32 K
conhost.exe	1	22624	612 K	0 K	0 K	300 K	912 K
svchost.exe	0	2304	3 532 K	0 K	0 K	356 K	3 888 K

3. Feladat CPU-Z

Megvizsgálta a gépben található CPU-t, leírta annak órajelét, feszültségét és hány mag helyezkedik el benne.

a, Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből



Nagyon sok hivatkozás történik egyszerre és mindegyik más-más függvény.

Fájlkezelésért, máskönyvtárból való behúzásért, megszakításért, és a lokalizációért felelnek

b, Milyen függőségei vannak a kernel32.dll-nek?

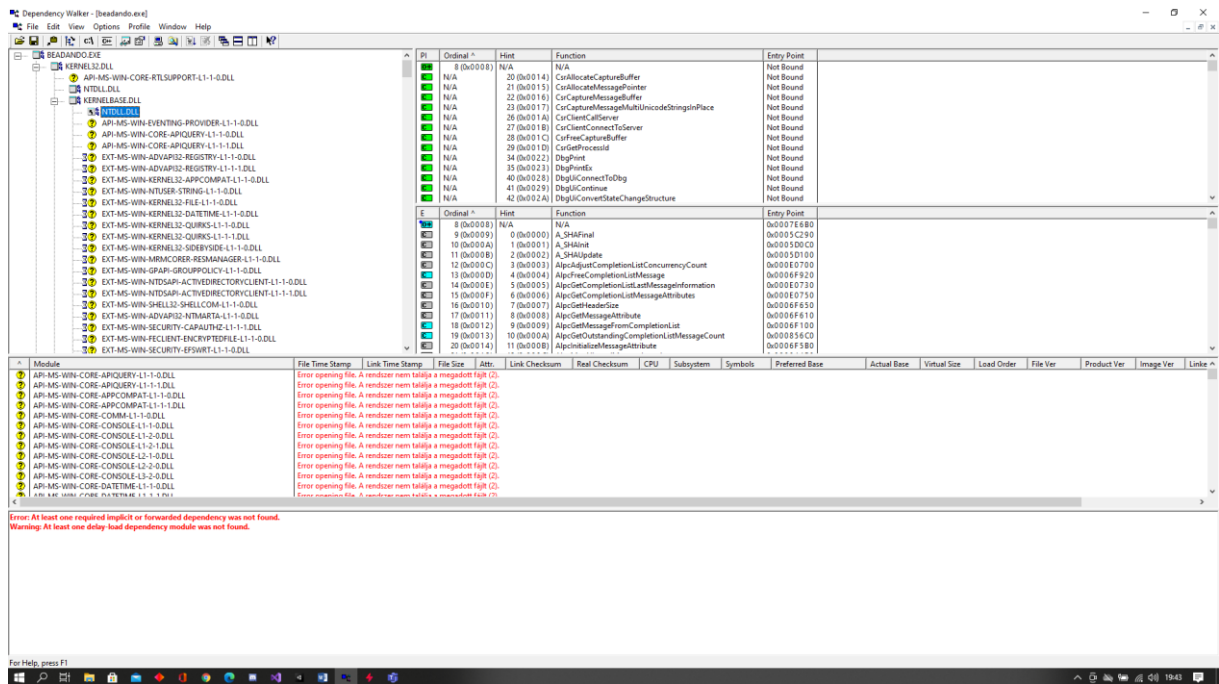
MS-WIN API-K

kernelbase.dll

ntdll.dll

rpcrt4.dll

c, Keresse meg NTDLL.DLL-t! Mi ennek a szerepe?



NTDLL.DLL egy dinamikus csatolású könyvtár, amely az NT kerneles függvényeket tartalmazza.