

Operációs rendszerek Bsc

3. gyak.

2021. 02. 24.

Készítette:

Takács Bálint Bsc
Programtervező
informatikus
P2GNFT

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>

SysinternalsSuite.zip

Fájl Parancsok Eszközök Kedvencek Opciók Súgó

Hozzáad Kicsomagolás ide Teszt Nézőke Töröl Keresés Varázsló Info Víruskeresés Megjegyzés SFX

↑ SysinternalsSuite.zip - ZIP archívum, kicsomagolt méret 100 392 646 byte

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	FFCA39E
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:...	33888E4F
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 fájl, 100 392 646 byte

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

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	R
[System Proc...	0	TCPV6	[2a01:36d:1400:6...	13518	[2a
[System Proc...	0	TCP	desktop-s13imh8	49215	52
[System Proc...	0	TCP	desktop-s13imh8	49605	85
ArmouryCrate...	4296	TCP	DESKTOP-S13IM...	9487	DE
ArmouryCrate...	4296	TCP	DESKTOP-S13IM...	9487	loc
ArmouryCrate...	4296	TCP	DESKTOP-S13IM...	13010	DE
ArmouryCrate...	14804	TCP	DESKTOP-S13IM...	13031	DE
ArmouryCrate...	14804	TCP	DESKTOP-S13IM...	13032	DE
ArmouryCrate...	14804	TCP	DESKTOP-S13IM...	17945	DE
ArmouryCrate...	14804	TCP	DESKTOP-S13IM...	61119	loc
ArmouryCrate...	14804	TCP	DESKTOP-S13IM...	61121	loc
ArmouryCrate...	4232	TCP	DESKTOP-S13IM...	7777	DE
ArmourySock...	16816	TCP	DESKTOP-S13IM...	9012	loc
ArmourySock...	16816	TCP	DESKTOP-S13IM...	61139	loc
ArmourySock...	16816	TCP	DESKTOP-S13IM...	9012	DE
ArmourySock...	16816	TCP	DESKTOP-S13IM...	9013	DE
ArmourySock...	16816	TCPV6	[0:0:0:0:0:0:0:0]	9012	[0:
ArmourySock...	16816	TCPV6	[0:0:0:0:0:0:0:0]	9013	[0:
asus_framework...	11600	TCP	DESKTOP-S13IM...	1042	DE
asus_framework...	11600	TCP	DESKTOP-S13IM...	1043	DE
asus_framework...	11600	TCP	DESKTOP-S13IM...	1043	loc
BitTorrent.exe	19004	TCP	DESKTOP-S13IM...	2914	loc
BitTorrent.exe	19004	TCP	DESKTOP-S13IM...	13518	DE
BitTorrent.exe	19004	UDP	DESKTOP-S13IM...	ssdp	*
BitTorrent.exe	19004	UDP	DESKTOP-S13IM...	13518	*

Endpoints: 343 Established: 86 Listening: 41 Time Wait: 54 Close Wait: 2

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

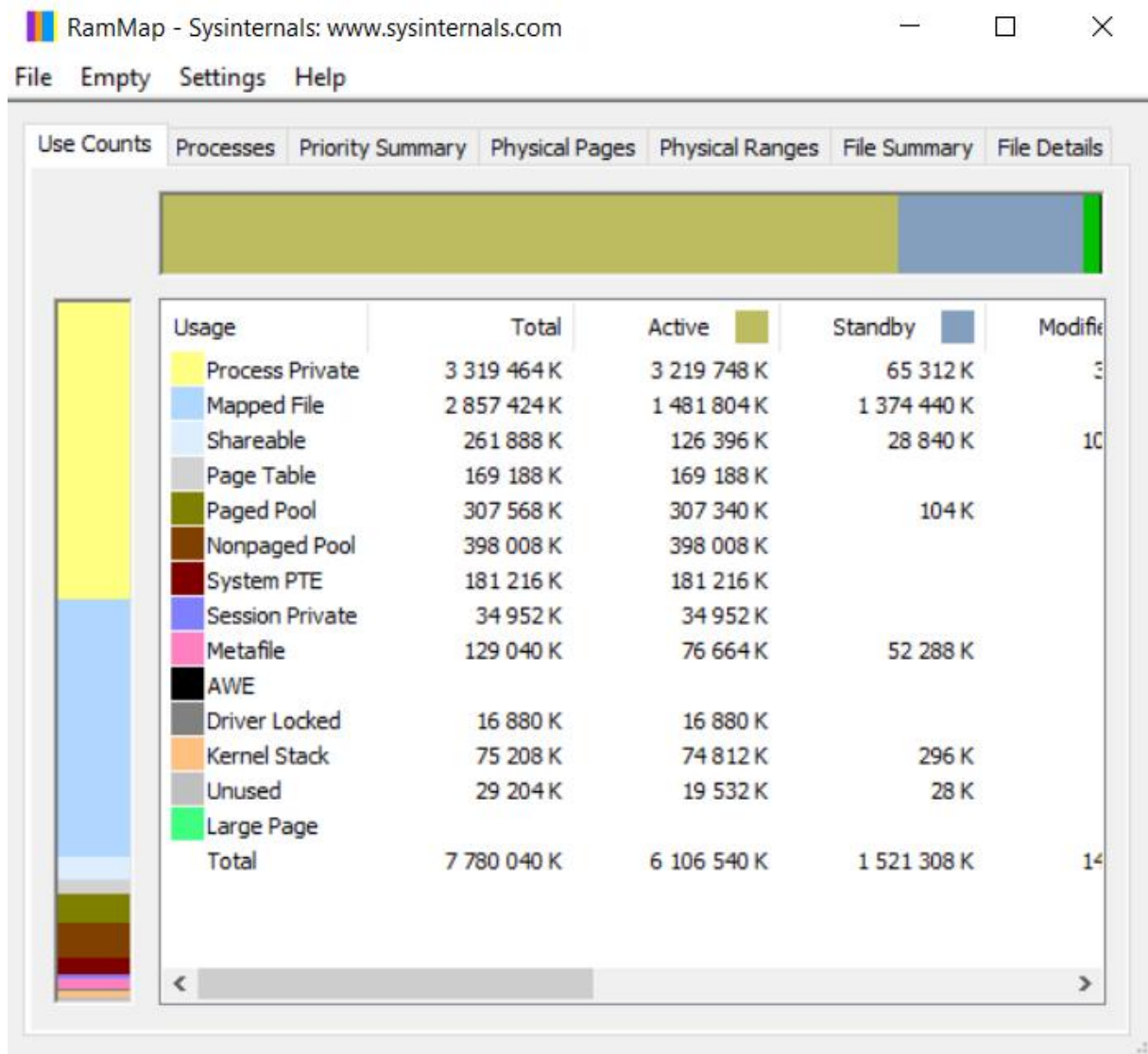
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-S13IMH8\Takács Bálint]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		10 728 K	39 912 K	172		
System Idle Process	95.22	60 K	8 K	0		
System	0.49	208 K	6 524 K	4		
Interrupts	0.24	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 072 K	1 016 K	604		
Memory Compression	< 0.01	720 K	96 936 K	2900		
csrss.exe	< 0.01	2 148 K	5 632 K	1016		
wininit.exe		1 588 K	6 640 K	1556		
services.exe	0.02	6 160 K	10 528 K	1680		
svchost.exe	0.08	15 220 K	34 248 K	1812	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPrvSE.exe		3 968 K	10 704 K	7456		
MoUsoCoreWorker.exe		41 420 K	51 484 K	17592		
StartMenuExperienceHost.exe		29 916 K	68 908 K	8428		
RuntimeBroker.exe		6 436 K	26 516 K	10440	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	87 688 K	87 236 K	16748	Search application	Microsoft Corporation
RuntimeBroker.exe		5 824 K	24 240 K	5332	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	27 348 K	12 500 K	15692	YourPhone	Microsoft Corporation
SettingSyncHost.exe		5 936 K	10 932 K	3488	Host Process for Setting Syn...	Microsoft Corporation
LockApp.exe	Susp...	15 816 K	43 288 K	5228	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		4 720 K	21 860 K	17136	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		9 800 K	35 288 K	1144	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2 740 K	14 824 K	13732	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	14 876 K	42 872 K	11992	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		2 940 K	18 148 K	17956	Runtime Broker	Microsoft Corporation
Cortana.exe	Susp...	30 112 K	56 000 K	1004	Cortana	Microsoft Corporation
RuntimeBroker.exe		4 648 K	24 852 K	19648	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2 144 K	10 348 K	10592	Runtime Broker	Microsoft Corporation
dllhost.exe		1 520 K	7 452 K	7004	COM Surrogate	Microsoft Corporation
SystemSettings.exe	Susp...	24 472 K	9 652 K	6672	Gépház	Microsoft Corporation
ApplicationFrameHost.exe	< 0.01	8 944 K	28 532 K	16820	Application Frame Host	Microsoft Corporation

CPU Usage: 4.78% Commit Charge: 52.93% Processes: 256 Physical Usage: 80.33%

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.

Fájl Nézet Riport Kedvencek Eszközök Súgó



Riport Vásárlás Eltávolítás BIOS frissítések Illesztőprogram frissítések

Menü Kedvencek

64 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 Desko...
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...

AIDA64 GPGPU Benchmark

— ×

☒ GPU1: nVIDIA GeForce GTX 1660 Ti
1590 MHz, 1536 cores, 24 CUs, Driver 461.09

☒ GPU2: AMD Radeon(TM) Graphics (gfx902)
1600 MHz, 448 cores, 7 CUs, Driver 3075.13 (PAL,HSAI)

☒ CPU: 8x ()
2900 MHz, 8 cores, 16 threads

	2 GPUs	x64 CPU
Memory Read	12833 MB/s	[TRIAL VERSION]
Memory Write	[TRIAL VERSION]	22330 MB/s
Memory Copy	261122 MB/s	19703 MB/s
Single-Precision FLOPS	7256 GFLOPS	[TRIAL VERSION]
Double-Precision FLOPS	269.0 GFLOPS	254.3 GFLOPS
24-bit Integer IOPS	7017 GIOPS	134.3 GIOPS
32-bit Integer IOPS	[TRIAL VERSION]	134.2 GIOPS
64-bit Integer IOPS	1366 GIOPS	66.15 GIOPS
AES-256	19357 MB/s	2830 MB/s
SHA-1 Hash	57100 MB/s	[TRIAL VERSION]
Single-Precision Julia	1967 FPS	[TRIAL VERSION]
Double-Precision Mandel	[TRIAL VERSION]	58.74 FPS

AIDA64 v5.98.4800 (c) 1995-2018 FinalWire Ltd.

Save

Results

Start Benchmark

Close

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.

 CPU-Z
 —
□
×

CPU | Caches | Mainboard | Memory | SPD | Graphics | Bench | About

Processor

Name	AMD Ryzen 7 Mobile 4800H				
Code Name	Renoir	Brand ID			
Package	Socket FP5				
Technology	7 nm	Core VID	1.250 V		
Specification	AMD Ryzen 7 4800H with Radeon Graphics				
Family	F	Model	0	Stepping	1
Ext. Family	17	Ext. Model	60	Revision	RN-A1
Instructions	MMX(+), SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, SSE4A, x86-64, AMD-V, AES, AVX, AVX2, FMA3, SHA				

Clocks (Core #0)

Core Speed	1397.17 MHz
Multiplier	x 14.0
Bus Speed	99.80 MHz
Rated FSB	

Cache

L1 Data	8 x 32 KBytes	8-way
L1 Inst.	8 x 32 KBytes	8-way
Level 2	8 x 512 KBytes	8-way
Level 3	2 x 4 MBytes	16-way

Selection

Socket #1

Cores

8

Threads

16

CPU-Z

Ver. 1.95.0.x64

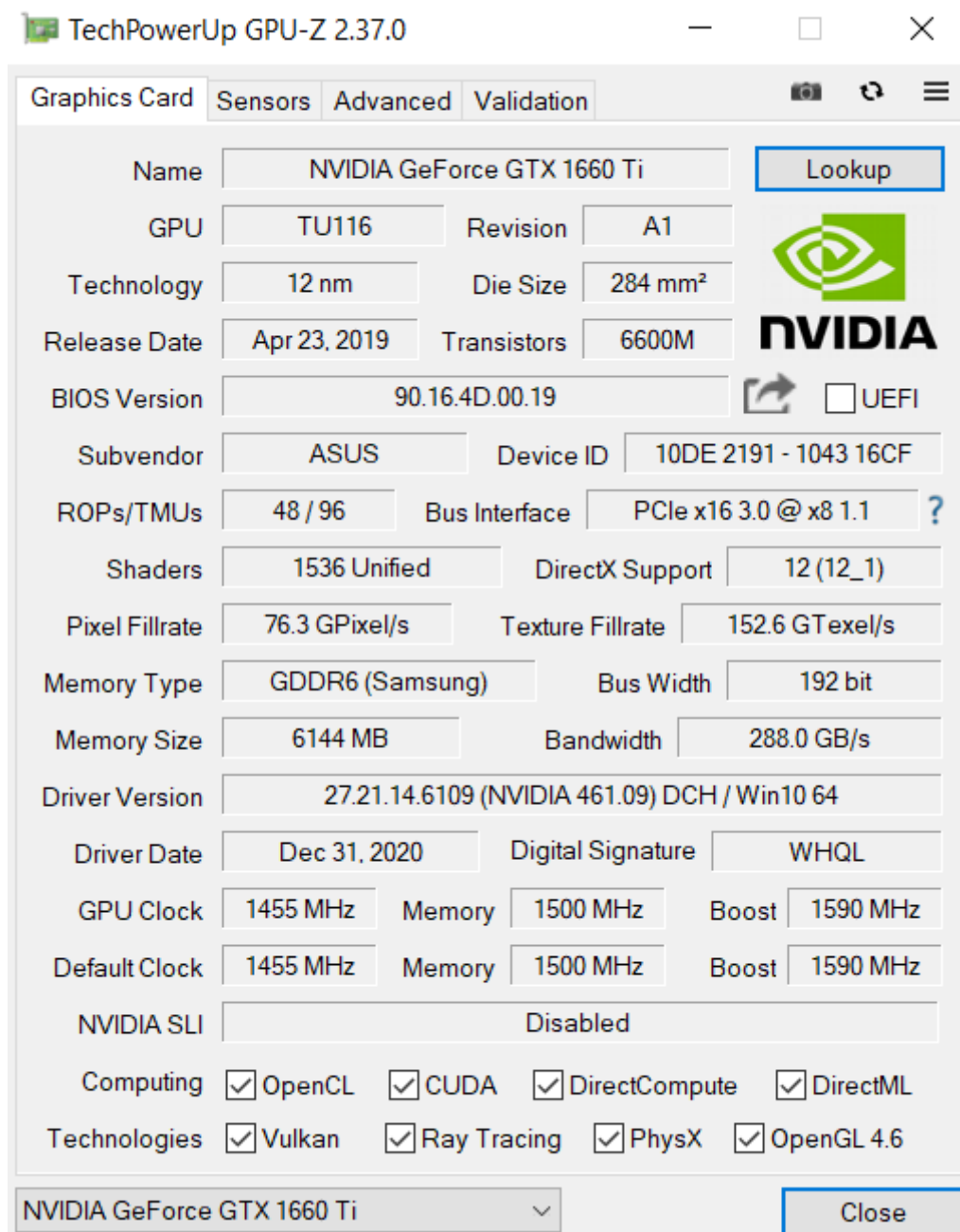
Tools

▼

Validate

Close

A CPU-Z program a processzoromról gyűjt ki adatokat.



A GPU-Z program a számítógépemben megtalálható grafikus meghajtóról vagyis a videokártyáról 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-COR
 ? 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

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
	N/A	12 (0x000C)	RtlPrintFunctionTable	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

Kernel32.dll API-MS-WIN-CORE-RTL NTDLL.dll KERNELBASE.dll NTDLL.dll API-MS-WIN-EVEN API-MS-WIN-COR API-MS-WIN-COR EXT-MS-WIN-ADV EXT-MS-WIN-ADV EXT-MS-WIN-KERN EXT-MS-WIN-KERN EXT-MS-WIN-KERN EXT-MS-WIN-KERN EXT-MS-WIN-KERN

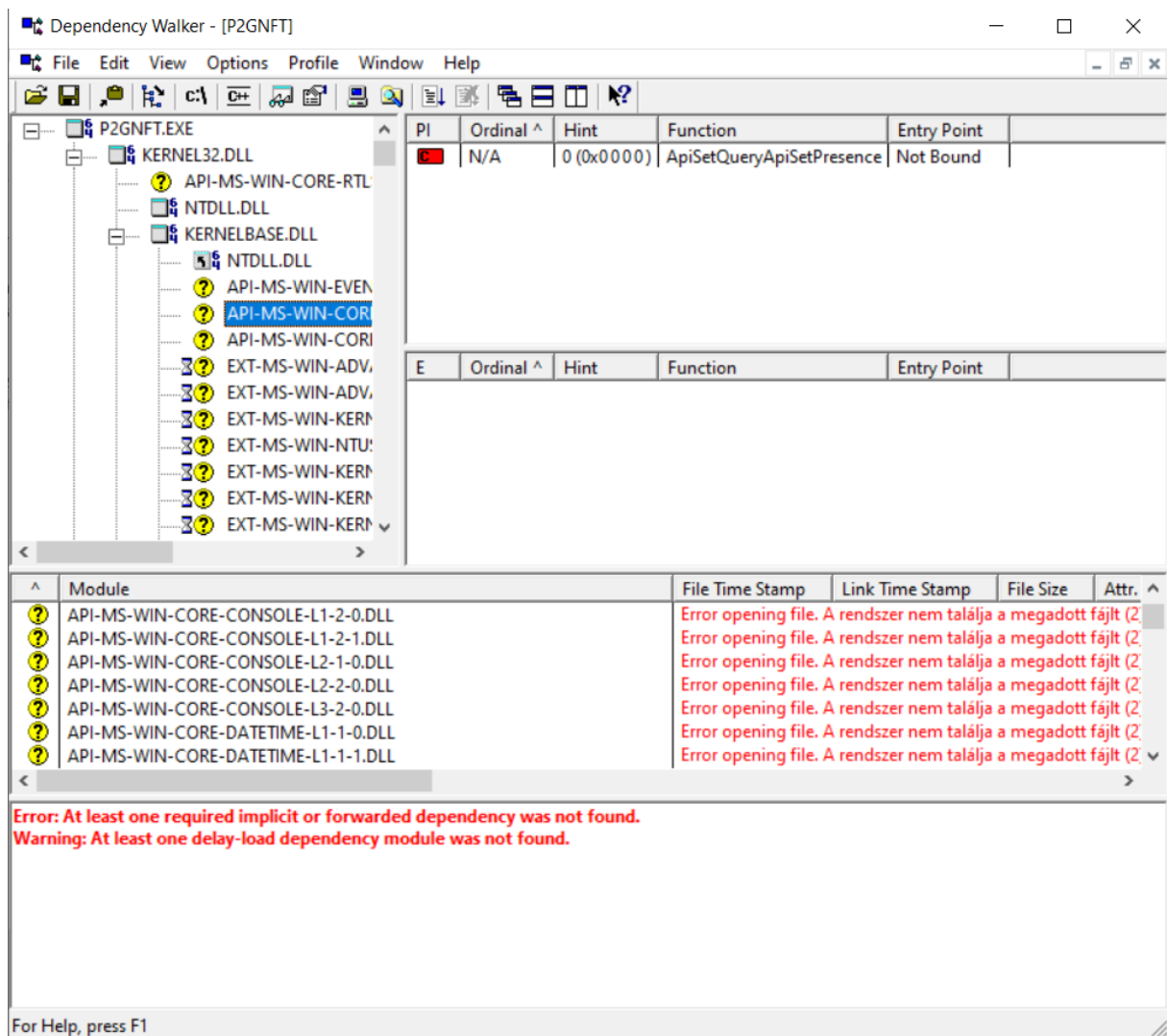
PI	Ordinal ^	Hint	Function	Entry Point
0	N/A	0 (0x0000)	EventActivityIdControl	Not Bound
3	N/A	3 (0x0003)	EventRegister	Not Bound
4	N/A	4 (0x0004)	EventSetInformation	Not Bound
5	N/A	5 (0x0005)	EventUnregister	Not Bound
9	N/A	9 (0x0009)	EventWriteTransfer	Not Bound

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	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!

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-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
20 (0x0014)	N/A	20 (0x0014)	CsrAllocateCaptureBuffer
21 (0x0015)	N/A	21 (0x0015)	CsrAllocateMessagePointer
23 (0x0017)	N/A	23 (0x0017)	CsrCaptureMessageMultiUnicodeStringsInPlace
24 (0x0018)	N/A	24 (0x0018)	CsrCaptureMessageString
26 (0x001A)	N/A	26 (0x001A)	CsrClientCallServer
28 (0x001C)	N/A	28 (0x001C)	CsrFreeCaptureBuffer
32 (0x0020)	N/A	32 (0x0020)	CsrVerifyRegion

E	Ordinal ^	Hint	Function
8 (0x0008)	N/A	N/A	N/A
9 (0x0009)	0 (0x0000)	0 (0x0000)	A_SHAFinal
10 (0x000A)	1 (0x0001)	1 (0x0001)	A_SHAInit
11 (0x000B)	2 (0x0002)	2 (0x0002)	A_SHAUpdate
12 (0x000C)	3 (0x0003)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount
13 (0x000D)	4 (0x0004)	4 (0x0004)	AlpcFreeCompletionListMessage
14 (0x000E)	5 (0x0005)	5 (0x0005)	AlpcGetCompletionListLastMessageInformation

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