

Operációs rendszerek BSc

2. Gyak.

2022. 02. 15.

Készítette:

Dávid Rebeka

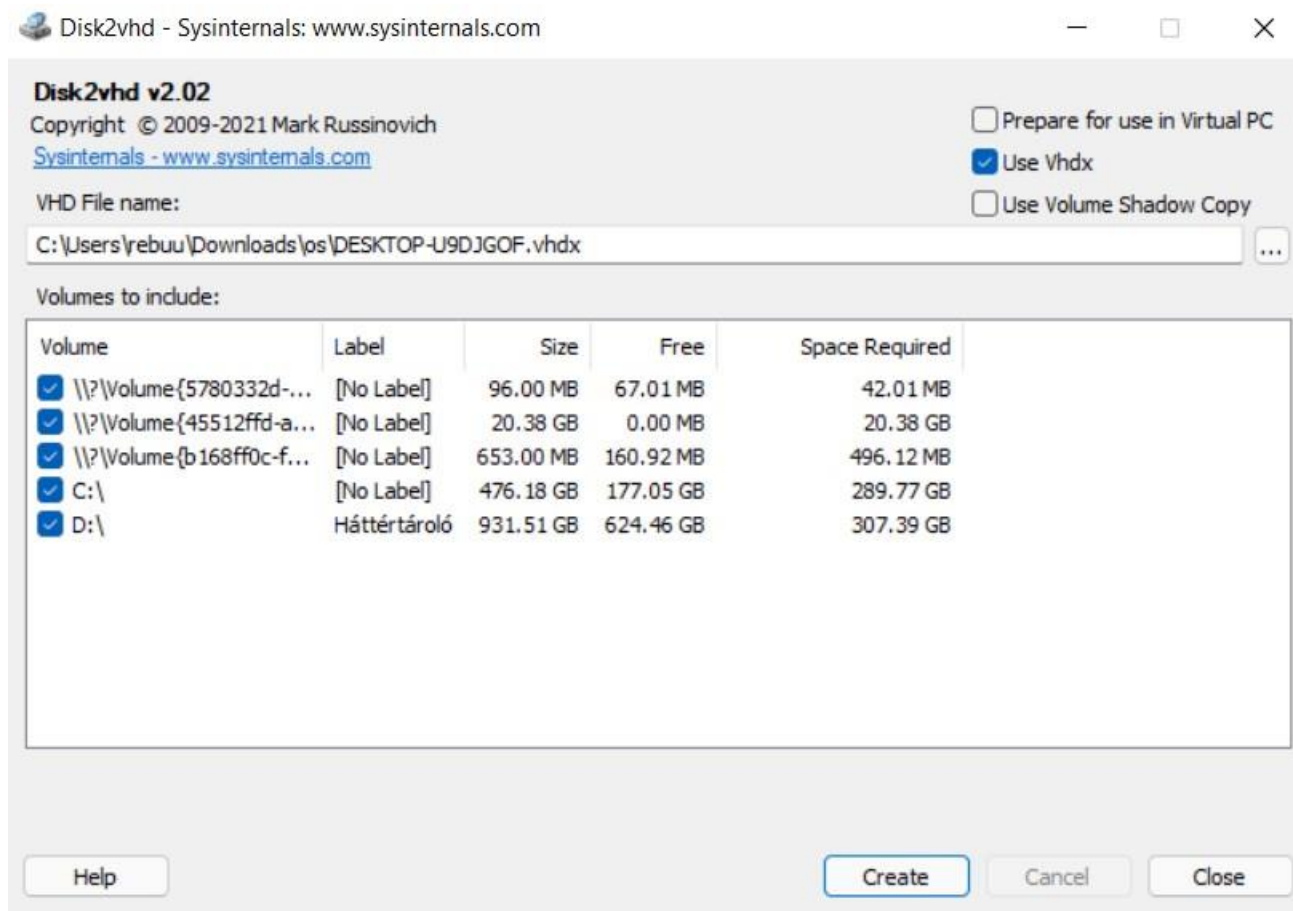
Programtervező informatikus

EQ4B3D

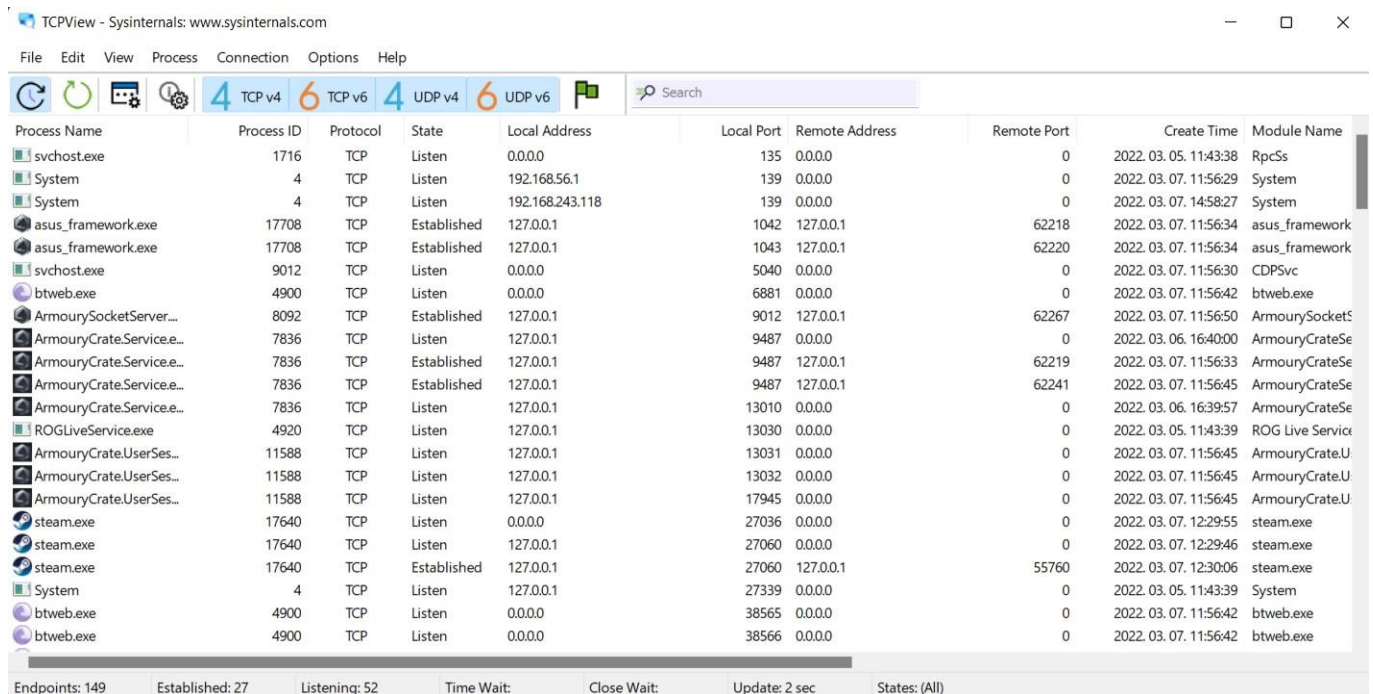
1. feladat

2. feladat

a, File and Disk Utilities (Disk2vhd)



b, Networking Utilities (TCPView)



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

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-U9DJGOF\rebuu]

The screenshot displays the Process Explorer window. The 'Process' list is expanded, showing various system and user processes. The columns include CPU, Private Bytes, Working Set, PID, Description, and Company Name. The 'System' tree on the left shows the hierarchy of processes. The status bar at the bottom indicates CPU Usage: 4.13%, Commit Charge: 46.48%, Processes: 222, and Physical Usage: 62.57%.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	94.91	60 K	8 K	0		
System	0.09	52 K	4 764 K	4		
smss.exe	0.09	104 K	1 156 K	696	via Hardware Interrupts and DPCs	
csrss.exe	< 0.01	1 612 K	258 524 K	3520		
csrss.exe		2 580 K	6 360 K	1132		
wininit.exe		1 516 K	6 372 K	1284		
services.exe		7 172 K	15 300 K	1400		
svchost.exe		17 924 K	32 324 K	1584	Windows-szolgalattasok gaz...	Microsoft Corporation
WmPrvSE.exe		31 360 K	40 020 K	8300		
dhhost.exe		3 556 K	11 012 K	14600		
unsecapp.exe		1 752 K	8 200 K	10580		
RuntimeBroker.exe		6 028 K	22 532 K	72592	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		16 900 K	55 368 K	15892	Runtime Broker	Microsoft Corporation
dhhost.exe		6 944 K	15 936 K	10868	COM Surrogate	Microsoft Corporation
ArmoryCrat.exe	Susp...	33 756 K	2 928 K	6508		
YourPhone.exe	Susp...	33 988 K	7 836 K	2224		Microsoft Corporation
RuntimeBroker.exe		5 700 K	12 984 K	4784	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		4 404 K	25 480 K	17400	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	40 972 K	5 684 K	7336	Desktop	Microsoft Corporation
ApplicationFrameHost.exe		18 680 K	35 680 K	5704	Application Frame Host	Microsoft Corporation
dhhost.exe		1 616 K	7 456 K	8540	COM Surrogate	Microsoft Corporation
Widgets.exe		7 324 K	33 448 K	14096		Microsoft Corporation
msedgeview2.exe	< 0.01	33 080 K	14 300 K	2384	Microsoft Edge WebView2	Microsoft Corporation
msedgeview2.exe		1 984 K	7 116 K	12340	Microsoft Edge WebView2	Microsoft Corporation
msedgeview2.exe		100 300 K	25 636 K	10612	Microsoft Edge WebView2	Microsoft Corporation
msedgeview2.exe		10 532 K	27 912 K	12980	Microsoft Edge WebView2	Microsoft Corporation
msedgeview2.exe		7 024 K	12 712 K	14416	Microsoft Edge WebView2	Microsoft Corporation
msedgeview2.exe		85 080 K	7 000 K	12388	Microsoft Edge WebView2	Microsoft Corporation
SearchHost.exe	Susp...	144 452 K	115 292 K	15384		Microsoft Corporation
StartMenuExperienceHost.exe		28 540 K	86 060 K	16665		
ShellExperienceHost.exe	Susp...	50 616 K	121 484 K	31100	Windows Shell Experience H...	Microsoft Corporation
MicrosoftPhotos.exe	Susp...	41 404 K	2 300 K	7516		
RuntimeBroker.exe		4 880 K	17 024 K	2124	Runtime Broker	Microsoft Corporation
MinSearchHost.exe	Susp...	23 480 K	73 828 K	13000		Microsoft Corporation
RuntimeBroker.exe		8 824 K	36 044 K	3016	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.exe		7 832 K	33 968 K	13344	System Settings Broker	Microsoft Corporation
dhhost.exe		1 380 K	13 456 K	13568	COM Surrogate	Microsoft Corporation
smartscreen.exe		8 108 K	23 940 K	11432	Windows Defender SmartScr...	Microsoft Corporation
dhhost.exe		3 276 K	14 788 K	7128	COM Surrogate	Microsoft Corporation
dhhost.exe		3 924 K	23 384 K	11796	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		6 764 K	30 068 K	8504	Runtime Broker	Microsoft Corporation
WUDFHost.exe		2 344 K	5 880 K	1668		

Process Monitor - Sysinternals: www.sysinternals.com

The screenshot displays the Process Monitor window. The 'Process Name' column is expanded, showing a list of events. The columns include Time, Process Name, PID, Operation, Path, Result, and Detail. The status bar at the bottom indicates 'Showing 101 669 of 233 321 events (43%)' and 'Backed by virtual memory'.

Time	Process Name	PID	Operation	Path	Result	Detail
15:15:41	svchost.exe	3708	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset 3 174 400, Le...
15:15:41	MsMpEng.exe	5132	ReadFile	C:\Windows\System32\ntdll.dll	SUCCESS	Offset 1 421 312, Le...
15:15:41	svchost.exe	3708	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset 704 512, Len...
15:15:41	MsMpEng.exe	5132	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset 15 798 272, L...
15:15:41	svchost.exe	3708	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset 692 224, Len...
15:15:41	MsMpEng.exe	5132	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset 15 081 472, L...
15:15:41	svchost.exe	3708	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset 647 168, Len...
15:15:41	MsMpEng.exe	5132	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset 15 736 832, L...
15:15:41	svchost.exe	3708	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive: False, Of...
15:15:41	MsMpEng.exe	5132	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset 15 720 448, L...
15:15:41	svchost.exe	3708	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset 638 976, Len...
15:15:41	svchost.exe	3708	QueryStandard...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 524...
15:15:41	MsMpEng.exe	5132	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset 14 946 304, L...
15:15:41	svchost.exe	3708	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset 123, Length: 1
15:15:41	MsMpEng.exe	5132	ReadFile	C:\Users\rebuu\Downloads\los\Procmon...	SUCCESS	Offset 1 310 720, Le...
15:15:41	lsass.exe	1440	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset 1 478 824, Le...
15:15:41	svchost.exe	3708	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive: False, Of...
15:15:41	svchost.exe	3708	QueryStandard...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 524...
15:15:41	svchost.exe	3708	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset 123, Length: 1
15:15:41	MsMpEng.exe	5132	ReadFile	C:\Users\rebuu\Downloads\los\Procmon...	SUCCESS	Offset 1 441 792, Le...
15:15:41	lsass.exe	1440	QueryNameInfo...	C:\Users\rebuu\Downloads\los\Procmon...	SUCCESS	Name: {Users\rebu...
15:15:41	lsass.exe	1440	QueryNameInfo...	C:\Users\rebuu\Downloads\los\Procmon...	SUCCESS	Name: {Users\rebu...
15:15:41	svchost.exe	3708	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive: False, Of...
15:15:41	svchost.exe	3708	QueryStandard...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 524...
15:15:41	svchost.exe	3708	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset 123, Length: 1
15:15:41	MsMpEng.exe	5132	ReadFile	C:\Users\rebuu\Downloads\los\Procmon...	SUCCESS	Offset 1 441 792, Le...
15:15:41	explorer.exe	9496	ReadFile	C:\Windows\System32\SHCore.dll	SUCCESS	Offset 882 616, Len...
15:15:41	explorer.exe	9496	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset 2 241 536, Le...
15:15:41	svchost.exe	3708	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive: False, Of...
15:15:41	svchost.exe	3708	QueryStandard...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 524...
15:15:41	svchost.exe	3708	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset 123, Length: 1
15:15:41	MsMpEng.exe	5132	ReadFile	C:\Users\rebuu\Downloads\los\Procmon...	SUCCESS	Offset 1 441 792, Le...
15:15:41	explorer.exe	9496	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
15:15:41	explorer.exe	9496	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
15:15:41	explorer.exe	9496	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND Desired Access R...	
15:15:41	explorer.exe	9496	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND Desired Access R...	
15:15:41	explorer.exe	9496	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:15:41	explorer.exe	9496	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
15:15:41	explorer.exe	9496	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:15:41	explorer.exe	9496	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND Desired Access R...	
15:15:41	svchost.exe	3708	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive: False, Of...
15:15:41	explorer.exe	9496	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND Desired Access R...	
15:15:41	svchost.exe	3708	QueryStandard...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 524...

Autoruns - Sysinternals: www.sysinternals.com

File Search Entry Options Category Help

WinLogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks Applnit Known DLLs

Autoruns Entry

Logon	Description	Publisher	Image Path	Timestamp	Virus Total
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Fri Feb 25 17:00:47 2022	
btweb	BitTorrent Web	(Verified) BitTorrent Inc	C:\Users\yebuu\AppData\Roaming\BitTorrent Web\btweb.exe	Tue Nov 30 23:43:58 2021	
Discord	Update	(Verified) Discord Inc	C:\Users\yebuu\AppData\Local\Discord\Update.exe	Tue Sep 21 19:16:42 2021	
EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.	C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\EpicGa...	Sat Feb 19 14:55:03 2022	
Steam	Steam	(Verified) Valve Corp.	C:\Program Files (x86)\Steam\steam.exe	Sat Mar 5 02:48:58 2022	
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sat Jun 5 14:11:05 2021	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Thu Feb 17 18:50:53 2022	
Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files\Google\Chrome\Application\98.0.4758.102\Installer\chrm...	Thu Feb 17 08:09:59 2022	
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\MicrosoftEdge\Application\99.0.1150.30\Installer\se...	Sat Mar 5 12:33:05 2022	
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Jun 5 14:06:26 2021	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				Thu Feb 17 18:51:15 2022	
ASUS Smart Display Control	ASUS Smart Display Control	(Verified) ASUSTEK COMPUTER INC.	C:\Program Files (x86)\ASUS\ASUS Smart Display Control\ASUSSmartDispla...	Fri Nov 27 11:28:18 2020	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				Thu Feb 17 18:51:14 2022	
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Jun 5 14:06:26 2021	
Explorer				Thu Mar 3 14:40:46 2022	
HKLM\SOFTWARE\Classes\Protocols\Filter				Thu Mar 3 14:36:49 2022	
text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Mi...	Thu Mar 3 14:40:46 2022	
HKLM\SOFTWARE\Classes\Protocols\Handler				Thu Mar 3 14:33:22 2022	
mso-minsb-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\MSCOSB.DLL	Thu Mar 3 14:33:22 2022	
mso-minsb.16	Microsoft Office component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\MSCOSB.DLL	Thu Mar 3 14:33:22 2022	
osf-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\MSCOSB.DLL	Thu Mar 3 14:33:22 2022	
osf.16	Microsoft Office component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\MSCOSB.DLL	Thu Mar 3 14:33:22 2022	
HKLM\Software\Classes\ShellEx\ContextMenuHandlers				Thu Feb 17 19:00:55 2022	
A\notepad++.64			File not found: C:\Program Files (x86)\Notepad++\NppShell_06.dll		
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	C:\Program Files\WinRAR\yarex.dll	Mon Jan 24 08:31:50 2022	

Ready

1°C Feihós

15:16 2022. 03. 07.

d, Security Utilities (LogonSession)

e, Information Utilities (RAMMap)

RamMap - Sysinternals: www.sysinternals.com

File Empty Settings Help

Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details

Usage	Total	Active	Standby	Modified	Modified ...	Transition	Zeroed	Free	Bad
Process Private	2 374 132 K	2 272 780 K	79 168 K	22 164 K		20 K			
Mapped File	3 528 744 K	930 412 K	2 597 864 K	468 K					
Shareable	220 900 K	131 668 K	1 884 K	87 348 K					
Page Table	131 668 K	131 668 K							
Paged Pool	339 968 K	339 612 K	196 K	160 K					
Nonpaged Pool	437 392 K	437 392 K							
System PTE	213 392 K	213 392 K							
Session Private	39 604 K	39 604 K							
Metafile	241 288 K	118 304 K	122 908 K		76 K				
AWIE									
Driver Locked	16 260 K	16 260 K		32 K					
Kernel Stack	65 160 K	65 068 K	60 K	12 K					
Unused	157 660 K	7 032 K	24 K				118 100 K	32 492 K	
Large Page									
Total	7 766 168 K	4 703 192 K	2 802 104 K	110 184 K	76 K	20 K	118 100 K	32 492 K	

1°C Feihós

15:17 2022. 03. 07.

3. feladat

a,

Dependency Walker - [eq4b3d]

File Edit View Options Profile Window Help

EQ4B3D.EXE

KERNEL32.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-2-2.DLL

NTDLL.DLL

KERNELBASE.DLL

NTDLL.DLL

API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL

API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL

EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL

EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL

EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-SIDEBYSIDE-L1-1-0.DLL

EXT-MS-WIN-MRM-CORER-RESMANAGER-L1-1-0.DLL

PI	Ordinal ^	Hint	Function	Entry Point
N/A		207 (0x00CF)	DeleteCriticalSection	Not Bound
N/A		236 (0x00EC)	EnterCriticalSection	Not Bound
N/A		279 (0x0117)	ExitProcess	Not Bound
N/A		300 (0x012C)	FindClose	Not Bound
N/A		304 (0x0130)	FindFirstFileA	Not Bound
N/A		321 (0x0141)	FindNextFileA	Not Bound
N/A		352 (0x0160)	FreeLibrary	Not Bound
N/A		388 (0x0184)	GetCommandLineA	Not Bound
N/A		510 (0x01FE)	GetLastError	Not Bound
N/A		529 (0x0211)	GetModuleHandleA	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
0x0001	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
0x0002	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
0x0003	3 (0x0003)	2 (0x0002)	ActivateActCtx	0x0001EE50
0x0004	4 (0x0004)	3 (0x0003)	ActivateActCtxWorker	0x00019BE0
0x0005	5 (0x0005)	4 (0x0004)	ActivatePackageVirtualizationContext	0x00023CF0
0x0006	6 (0x0006)	5 (0x0005)	AddAtomA	0x000577D0
0x0007	7 (0x0007)	6 (0x0006)	AddAtomW	0x000080F0
0x0008	8 (0x0008)	7 (0x0007)	AddConsoleAliasA	0x00023A00
0x0009	9 (0x0009)	8 (0x0008)	AddConsoleAliasW	0x00023A10
0x000A	10 (0x000A)	9 (0x0009)	ΔΔΔΔΔΔΔΔΔΔ	api-ms-win-core-libloader-l1-1-0 ΔΔΔΔΔΔΔΔΔΔ

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL						Error opening file. A rendszert nem találja a megadott fájl (2).						
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL						Error opening file. A rendszert nem találja a megadott fájl (2).						
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL						Error opening file. A rendszert nem találja a megadott fájl (2).						
API-MS-WIN-CORE-COMM-L1-1-0.DLL						Error opening file. A rendszert nem találja a megadott fájl (2).						
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL						Error opening file. A rendszert nem találja a megadott fájl (2).						
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL						Error opening file. A rendszert nem találja a megadott fájl (2).						
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL						Error opening file. A rendszert nem találja a megadott fájl (2).						
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL						Error opening file. A rendszert nem találja a megadott fájl (2).						
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL						Error opening file. A rendszert nem találja a megadott fájl (2).						

Error: At least one required implicit or forwarded dependency was not found.
Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.

For Help, press F1

2°C Felhős

15:38

2022. 03. 07.