

Jegyzőkönyv Operációs rendszerek

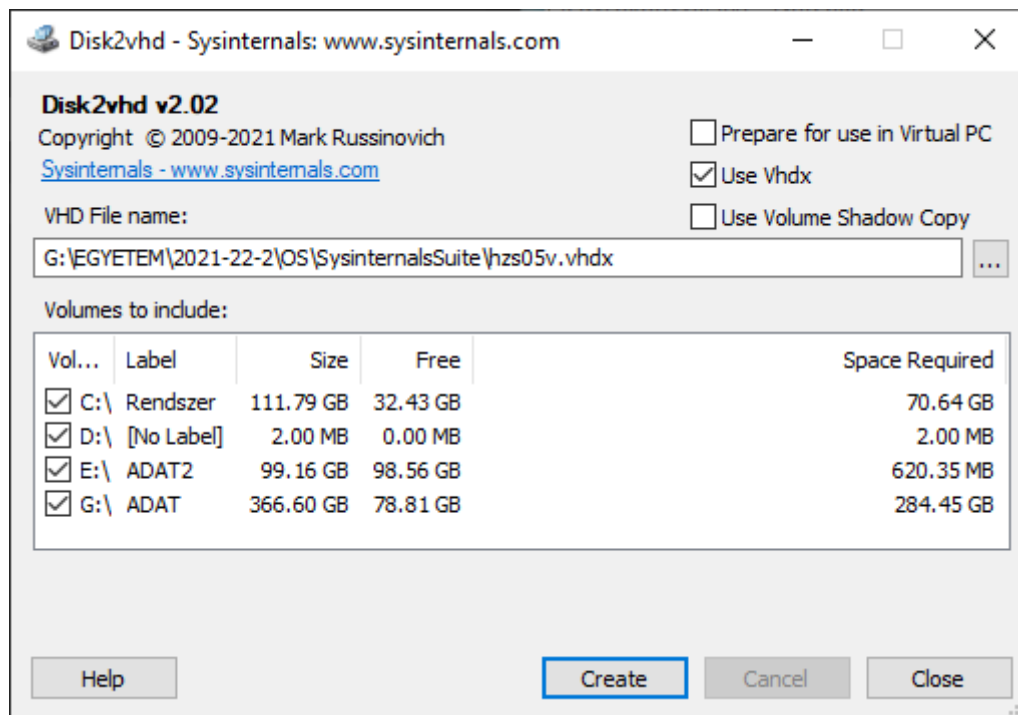
2. gyakorlat

2.feladat

Timkó András
HVS05V
ge-BGI

a) File and Disk Utilities (Disk2vhd)

A Disk2vhd egy olyan segédprogram, amely létrehozza a fizikai lemezek VHD-verzióit. Virtuális lemezt, amit a virtuális gépek tudnak használni.



b) Networking Utilities (TCPView)

A TCPView egy Windows program, amely részletes listában mutatja be a rendszer összes TCP- és UDP-végpontját, beleértve a helyi és távoli címeket, valamint a TCP-kapcsolatok állapotát.


A parancssori netstathoz hasonlít.

TCPView - Sysinternals: www.sysinternals.com						
File Edit View Process Connection Options Help						
4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search						
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote
svchost.exe	640	TCP	Listen	0.0.0.0	135	0.0.0.0
System	4	TCP	Listen	192.168.0.31	139	0.0.0.0
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0
svchost.exe	6352	TCP	Listen	0.0.0.0	5040	0.0.0.0
System	4	TCP	Listen	127.0.0.1	28385	0.0.0.0
System	4	TCP	Listen	127.0.0.1	28390	0.0.0.0
lsass.exe	936	TCP	Listen	0.0.0.0	49664	0.0.0.0
wininit.exe	812	TCP	Listen	0.0.0.0	49665	0.0.0.0
svchost.exe	1716	TCP	Listen	0.0.0.0	49666	0.0.0.0
svchost.exe	1336	TCP	Listen	0.0.0.0	49667	0.0.0.0
spoolsv.exe	3020	TCP	Listen	0.0.0.0	49668	0.0.0.0
services.exe	900	TCP	Listen	0.0.0.0	49681	0.0.0.0
svchost.exe	3612	TCP	Established	192.168.0.31	56511	20.199.1
chrome.exe	2388	TCP	Established	192.168.0.31	56653	142.250.
chrome.exe	2388	TCP	Established	192.168.0.31	56657	142.250.
chrome.exe	2388	TCP	Established	192.168.0.31	56769	54.85.24
svchost.exe	11620	TCP	Established	192.168.0.31	56798	20.54.23
[Time Wait]		TCP	Time Wait	127.0.0.1	56799	127.0.0.1
[Time Wait]		TCP	Time Wait	192.168.0.31	56800	20.49.15
<						
Endpoints: 83		Established: 5		Listening: 24		Time Wait: 2
				Close Wait:		Update: 2 sec












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

AutoRuns Ez a segédprogram, amely a legátfogóbb ismeretekkel rendelkezik az indítási figyelők automatikus indítási helyéről, megmutatja, milyen programok futtatására van konfigurálva a rendszerindítás vagy a bejelentkezés során, és mikor indít el különböző beépített Windows-alkalmazásokat, például az Internet Explorer-t, az Explorer-t és a médialejátszókat.

Megfigyeli hogy melyik program indításakor milyen más program vagy programrész indul el. Malware megtalálásához is használható.

 Autoruns - Sysinternals: www.sysinternals.com

File Search Entry Options Category Help

Known DLLs WinLogon Winsock Providers Print Monitors

Everything Logon Explorer Internet Explorer Scheduled Tasks

Autoruns Entry Description Publisher

Logon

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Entry	Description	Publisher
<input checked="" type="checkbox"/> Discord	Update	(Verified)
<input checked="" type="checkbox"/> Feem		(Not Verif
<input checked="" type="checkbox"/> MouseServer		
<input checked="" type="checkbox"/> Steam	Steam	(Verified)

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Entry	Description	Publisher
<input checked="" type="checkbox"/> AdobeAAMUpdater-1.0	Adobe Updater Startup Utility	(Verified)
<input checked="" type="checkbox"/> AdobeGCInvoker-1.0	Adobe GC Invoker Utility	(Verified)
<input checked="" type="checkbox"/> IAStorIcon	Delayed launcher	(Not Verif
<input checked="" type="checkbox"/> RtsCM	Integrated Camera Preview Rotation Helper	(Verified)

HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell

Entry	Description	Publisher
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified)


HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components

Entry	Description	Publisher
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified)
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified)
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified)

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

Entry	Description	Publisher
<input checked="" type="checkbox"/> Acrobat Assistant 8.0	AcroTray	(Verified)
<input checked="" type="checkbox"/> Adobe ARM		(Not Verif
<input checked="" type="checkbox"/> Intel Driver & Support Assistant	Intel Driver & Support Assistant Tray	(Verified)
<input checked="" type="checkbox"/> OI RController	OI RController	(Verified)

<

 Discord
Update
(Verified) Discord Inc.
C:\Users\Xanax\AppData\Local\Discord\Update.exe --processStart Discord.exe

Size: 1,477 K
Time: Thu Dec 3 22:43:28 2020
Version: 1.1.1.0

Ready

Processexplorer

A Folyamatkezelő megmutatja, hogy mely leírókat és DLL-folyamatokat nyitották meg vagy töltötték be.

Főbb jellemzői:

Az aktív folyamatok felügyelete

A folyamatok magatartáskezelése

Egy adott folyamat részletes információinak megtekintése

CPU, GPU, RAM, I / O adatok megjelenítése a grafikonokon

Process Explorer - Sysinternals: www.sysinternals.com [XANAX\Xanax]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Susp...	184 K	23,308 K	56		
Registry		8,040 K	47,660 K	104		
System Idle Process	86.44	60 K	8 K	0		
System	0.38	192 K	100 K	4		
Interrupts	0.38	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,068 K	1,012 K	392		
Memory Compression		492 K	41,408 K	2008		
csrss.exe	< 0.01	2,072 K	3,960 K	556		
wininit.exe		1,700 K	4,436 K	812		
services.exe		6,960 K	9,684 K	900		
svchost.exe		15,904 K	24,748 K	480	Host Process for Windows S...	Microsoft Corporation
unsecapp.exe		2,448 K	4,648 K	4676		
WmiPrvSE.exe		4,240 K	8,892 K	5152		
MoUsocoreWorker.exe		23,248 K	37,124 K	7860		
SettingSyncHost.exe		5,260 K	7,252 K	4616	Host Process for Setting Syn...	Microsoft Corporation
StartMenuExperience...		29,068 K	70,240 K	9752		
RuntimeBroker.exe		5,792 K	24,204 K	10452	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	144,048 K	209,848 K	9076	Search application	Microsoft Corporation
TextInputHost.exe		14,492 K	43,360 K	7500		Microsoft Corporation
RuntimeBroker.exe		9,572 K	36,000 K	4724	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	33,648 K	18,380 K	10408		Microsoft Corporation
RuntimeBroker.exe		4,560 K	19,508 K	13308	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3,172 K	21,468 K	9500	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	25,724 K	3,400 K	10908	Settings	Microsoft Corporation
ApplicationFrameHost...		8,044 K	28,356 K	9664	Application Frame Host	Microsoft Corporation
UserOOBEBroker.exe		1,844 K	10,060 K	10832	User OOBEBroker	Microsoft Corporation
ShellExperienceHost....	Susp...	20,140 K	58,656 K	11348	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		5,304 K	19,652 K	11976	Runtime Broker	Microsoft Corporation
dllhost.exe		4,248 K	13,404 K	7720	COM Surrogate	Microsoft Corporation
smartscreen.exe		8,348 K	24,800 K	10840	Windows Defender SmartScr...	Microsoft Corporation
svchost.exe	0.38	14,676 K	18,284 K	640	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,028 K	6,428 K	692	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,160 K	2,208 K	1152	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,616 K	7,260 K	1280	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,228 K	11,384 K	1336	Host Process for Windows S...	Microsoft Corporation
taskhostw.exe		7,220 K	17,636 K	12616	Host Process for Windows T...	Microsoft Corporation
RAVBg64.exe		4,048 K	4,760 K	2512	HD Audio Background Proc...	Realtek Semiconducto
svchost.exe		3,240 K	6,428 K	1364	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 13.45% Commit Charge: 43.87% Processes: 190 Physical Usage: 45.16%

Processmonitor

A Folyamatfigyelő egy fejlett monitorozási eszköz Windows, amely valós idejű fájlrendszer-, beállításjegyzék- és folyamat- / száltevékenységet mutat be. Ezeket leállíthatjuk, módosíthatjuk a prioritásukat, jellemzőit, vagy vizuálisan láthatjuk gépünk működését a monitor ablak segítségével.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ... Process Name PID Operation Path

19:12:...	Explorer.EXE	8328	RegQueryValue	HKCR\inifile
19:12:...	csrss.exe	7072	RegQueryValue	HKLM
19:12:...	Explorer.EXE	8328	QueryStandard...	C:\Users\Xanax\AppData\Local\Microsoft\Windows\Explorer\...
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\inifile\DocObject
19:12:...	csrss.exe	7072	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide\...
19:12:...	csrss.exe	7072	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\...
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\SystemFileAssociations\text
19:12:...	csrss.exe	7072	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\...
19:12:...	csrss.exe	7072	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\...
19:12:...	Explorer.EXE	8328	RegOpenKey	HKCR\SystemFileAssociations\text
19:12:...	csrss.exe	7072	RegOpenKey	HKCU\Software\Classes\SystemFileAssociations\text
19:12:...	csrss.exe	7072	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\...
19:12:...	csrss.exe	7072	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\...
19:12:...	Explorer.EXE	8328	QueryStandard...	C:\Users\Xanax\AppData\Local\Microsoft\Windows\Explorer\...
19:12:...	csrss.exe	7072	RegQueryValue	HKCR\SystemFileAssociations\text\DocObject
19:12:...	csrss.exe	7072	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\...
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\SystemFileAssociations\text
19:12:...	csrss.exe	7072	QueryStandard...	C:\Users\Xanax\AppData\Local\Microsoft\Windows\Explorer\...
19:12:...	csrss.exe	7072	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\...
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\SystemFileAssociations\text
19:12:...	Explorer.EXE	8328	RegOpenKey	HKCR\SystemFileAssociations\text
19:12:...	csrss.exe	7072	RegOpenKey	HKCU\Software\Classes\SystemFileAssociations\text\DocObject
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\SystemFileAssociations\text
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\SystemFileAssociations\text\DocObject
19:12:...	csrss.exe	7072	QueryStandard...	C:\Users\Xanax\AppData\Local\Microsoft\Windows\Explorer\...
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\inifile
19:12:...	csrss.exe	7072	RegOpenKey	HKCU\Software\Classes\inifile
19:12:...	csrss.exe	7072	RegQueryValue	HKCR\inifile\BrowseInPlace
19:12:...	csrss.exe	7072	CreateFile	C:\Windows\WinSxS\Manifests\amd64_microsoft.windows.c...
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\inifile
19:12:...	csrss.exe	7072	QueryNetwork...	C:\Windows\WinSxS\Manifests\amd64_microsoft.windows.c...
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\inifile
19:12:...	csrss.exe	7072	CreateFile	C:\Windows\WinSxS\Manifests\amd64_microsoft.windows.c...
19:12:...	csrss.exe	7072	RegOpenKey	HKCU\Software\Classes\inifile\BrowseInPlace
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\inifile
19:12:...	csrss.exe	7072	RegOpenKey	HKCR\inifile\BrowseInPlace

Showing 129,455 of 423,992 events (30%) Backed by virtual memory

Process Tree

☐ Only show processes still running at end of current trace
☒ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Comr
svchost.exe (10544)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	XANAX\Xanax	C\Wi
svchost.exe (2684)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	XANAX\Xanax	C\Wi
svchost.exe (1860)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	XANAX\Xanax	C\Wi
svchost.exe (12744)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	XANAX\Xanax	C\Wi
svchost.exe (4412)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C\Wi
svchost.exe (9696)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C\Wi
svchost.exe (6844)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C\Wi
lsaiso.exe (912)	Credential Guard ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	??C
lsass.exe (936)	Local Security Aut...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C\Wi
fontdrvhost.exe (504)	Usermode Font Dr...	C:\Windows\syst...		Microsoft Corporat...	Font Driver Host...	*fontc
csrss.exe (7072)	Client Server Runt...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	%Syst
WinLogon.exe (6388)	Windows Log-on ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C\Wi
fontdrvhost.exe (5356)	Usermode Font Dr...	C:\Windows\Syst...		Microsoft Corporat...	Font Driver Host...	*fontc
dwm.exe (8764)	Desktop Window ...	C:\Windows\Syst...		Microsoft Corporat...	Window Manager...	*dwm
igfxHK.exe (12552)	igfxHK Module	C:\Windows\syst...		Intel Corporation	XANAX\Xanax	igfxHI
igfxTray.exe (3500)		C:\Windows\syst...			XANAX\Xanax	igfxTr
SYNTPHELPER.EXE (4368)	Synaptics Pointing...	C:\PROGRAM FI...		Synaptics Incorpo...	XANAX\Xanax	C\P
Explorer.EXE (8328)	Windows Explorer	C:\Windows\Expl...		Microsoft Corporat...	XANAX\Xanax	C\W

Description: Windows Explorer
Company: Microsoft Corporation
Path: C:\Windows\Explorer.EXE
Command: C:\Windows\Explorer.EXE
User: XANAX\Xanax
PID: 8328 Started: 19/02/2022 17:19:43

Go To Event Include Process Include Subtree Close

d) Security Utilities (LogonSession)

Felsorolja a jelenleg aktív bejelentkezési munkameneteket, és ha megadja a -p beállítást, az egyes munkamenetekben futó folyamatokat.

C:\> Administrator: Command Prompt

```
G:\EGYETEM\2021-22-2\OS\SysinternalsSuite>logonsessions64.exe -p
```

```
LogonSessions v1.41 - Lists logon session information  
Copyright (C) 2004-2020 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
[0] Logon session 00000000:000003e7:  
    User name:      WORKGROUP\XANAX$  
    Auth package:   NTLM  
    Logon type:     (none)  
    Session:       0  
    Sid:           S-1-5-18  
    Logon time:     13/02/2022 13:33:35  
    Logon server:  
    DNS Domain:  
    UPN:  
        912: LsaIso.exe  
        936: lsass.exe  
        480: svchost.exe  
        692: svchost.exe  
        1152: svchost.exe  
        1280: svchost.exe  
        1336: svchost.exe  
        1364: svchost.exe  
        1384: svchost.exe  
        1576: svchost.exe  
        1884: svchost.exe  
        1896: svchost.exe  
        1976: svchost.exe  
        1052: igfxCUIService.exe  
        2068: svchost.exe  
        2184: svchost.exe  
        2256: svchost.exe  
        2280: svchost.exe  
        2868: svchost.exe
```

e) Information Utilities (RAMMap)

A RAMMap egy speciális fizikai memóriahasználat-elemzési segédprogram. Különböző módokon mutatja be a használati adatokat a különböző lapjain:

A Darabszámok használata: használati adatok összegzése típus és lapozási lista szerint Folyamatok: a munkakészletek méretének feldolgozása

Prioritás összegzése: rangsorolások készletlistaméretei

Fizikai lapok: oldalankénti használat az összes fizikai memóriához

Fizikai tartományok: fizikai memóriacímek

Fájl összegzése: fájl adatok a RAM-ban fájl szerint

Fájl részletei: egyes fizikai lapok fájl szerint

