

Operációs rendszerek BSc

3. gyak

2021.02.24.

Készítette:

Ferencsik Márk BSc

Programtervező informatika

UJTWLL

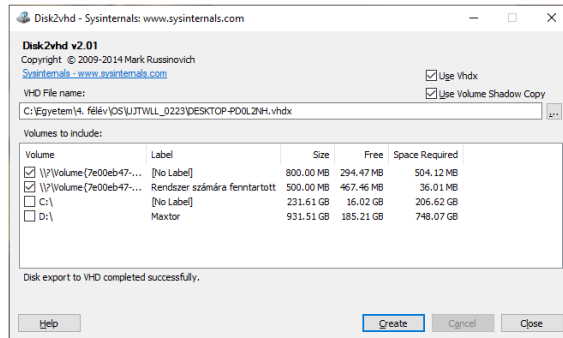
1. Windows belső működésének tanulmányozása:

Sysinternals Suite fájlcsomag letöltésre került.

2. Sysinternals néhány programjának futtatása:

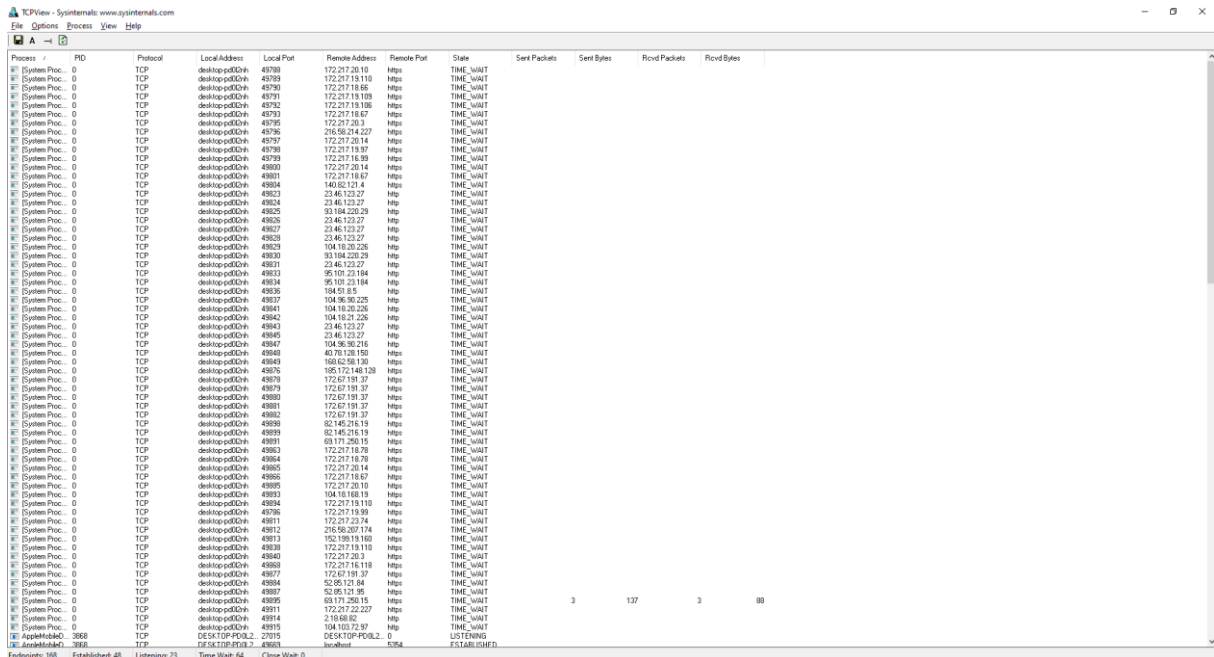
a. File and Disk Utilities:

Célja egy lemezképfájl létrehozása adott meghajtó(k)ról.



b. Networking Utilities:

Célja a processzekhez tartozó hálózati kapcsolatok adatainak összesítése.



c. Process Utilities:

Célja a processzek és adatainak listázása.

Process Monitor - Sysinternals.com www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
18:44...	svchost.exe	2228	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 659 688; Le...
18:44...	svchost.exe	2228	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 659 688; Le...
18:44...	svchost.exe	2228	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 659 904; Le...
18:44...	svchost.exe	2228	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: Fals...
18:44...	svchost.exe	2228	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124. Length...
18:44...	svchost.exe	2228	ReadFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: Fals...
18:44...	svchost.exe	2228	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124. Length...
18:44...	Explorer.EXE	920	ReadFile	C:\Windows\System32\shimapi.dll	SUCCESS	Offset: 312 832; S...
18:44...	McMpfEng.exe	3268	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 942 208...
18:44...	McMpfEng.exe	8808	ReadFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Offset: 210 432; L...
18:44...	McMpfEng.exe	3268	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 446 592...
18:44...	McMpfEng.exe	8808	ReadFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Offset: 187 904; L...
18:44...	McMpfEng.exe	3268	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 151 680...
18:44...	svchost.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Sof...	SUCCESS	Offset: 1 038 336...
18:44...	svchost.exe	2228	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: Fals...
18:44...	svchost.exe	2228	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124. Length...
18:44...	svchost.exe	2228	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 104. Length...
18:44...	svchost.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Sof...	SUCCESS	Offset: 1 021 952...
18:44...	svchost.exe	3268	LockFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: Fals...
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Name
18:44...	McMpfEng.exe	3268	UnlockFileSingle	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 124. Length...
18:44...	McMpfEng.exe	3268	LockFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: Fals...
18:44...	McMpfEng.exe	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Handle Tag...
18:44...	McMpfEng.exe	3268	LockFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: True, Of...
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Handle Tag...
18:44...	Explorer.EXE	920	RegOpenKey	C:\Program Files\Logitech Gaming Sof...	SUCCESS	Offset: 3 658 912...
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND Desired Access: R...	
18:44...	Explorer.EXE	920	RegOpenKey	HICR\Applications\Promoon64.exe	NAME NOT FOUND Desired Access: R...	
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Name
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Handle Tag...
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Offset: 3 658 912...
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND Desired Access: R...	
18:44...	McMpfEng.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Sof...	SUCCESS	Offset: 5 403 648...
18:44...	Explorer.EXE	920	RegOpenKey	HICR\Applications\Promoon64.exe	NAME NOT FOUND Desired Access: R...	
18:44...	McMpfEng.exe	3268	RegOpenKey	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 658 912...
18:44...	McMpfEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 654 496...
18:44...	McMpfEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 658 952...
18:44...	McMpfEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 658 616...
18:44...	McMpfEng.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Sof...	SUCCESS	Offset: 5 342 208...
18:44...	McMpfEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 658 912...
18:44...	McMpfEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 662 736...
18:44...	McMpfEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 666 832...
18:44...	McMpfEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 666 896...
18:44...	McMpfEng.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Sof...	SUCCESS	Offset: 5 379 072...

The screenshot shows the Autoruns application window with the 'Logon' tab active. The interface includes a menu bar (File, Entry, Options, Help), a toolbar with icons for Known DLLs, Logon, Explorer, Winsock Providers, Internet Explorer, Print Monitors, Services, Drivers, Network Providers, Boot Execute, WMI, Image Hijacks, and Office AppInit. A 'Filter' text box is at the top. The main table lists startup items with columns for 'Autorun Entry', 'Description', 'Publisher', 'Image Path', 'Timestamp', and 'Virus Total'. The list contains entries for system files (e.g., 'cmd.exe', 'Launch LCore'), services (e.g., 'Perfstart Service'), and various user applications (e.g., 'Teams', 'Opera Browser Assistant', 'Skype for Desktop', 'Wargaming.net Game Center', 'Kildes a/z OneNote pro...'). The 'Virus Total' column shows links to VirusTotal for many entries.

d. Security Utilities:

Célja a bejelentkezési időszakok adatainak listázása.

```
Kijelölte Administrator Parancsok
C:\Vegyes\4. feladat\Uj\Uj\Uj_0223\logonsessions64.exe

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

[0] Logon session 00000000-00000007:
User name: WORKGROUP\DESKTOP-P0BL2M$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 2021. 03. 02. 18:40:56
Logon server:
DNS Domain:
UPN:

[1] Logon session 00000000-00000007:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 2021. 03. 02. 18:40:56
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000-00000007:
User name: Font Driver Host\UMFD-0
Auth package: Negotiate
Logon type: Interactive
Session: 0
Sid: S-1-5-96-0-0
Logon time: 2021. 03. 02. 18:40:56
Logon server:
DNS Domain:
UPN:

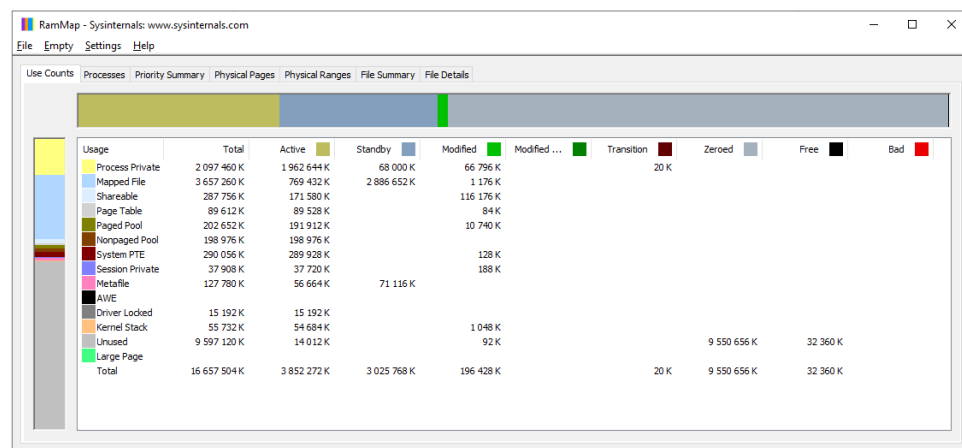
[3] Logon session 00000000-00000007:
User name: Font Driver Host\UMFD-1
Auth package: Negotiate
Logon type: Interactive
Session: 1
Sid: S-1-5-96-0-1
Logon time: 2021. 03. 02. 18:40:56
Logon server:
DNS Domain:
UPN:

[4] Logon session 00000000-00000007:
User name: WORKGROUP\DESKTOP-P0BL2M$
Auth package: Negotiate
Logon type: Service
Session: 0
Sid: S-1-5-20
Logon time: 2021. 03. 02. 18:40:57
Logon server:
DNS Domain:
UPN:

[5] Logon session 00000000-00010002:
```

e. Information Utilities:

Célja a számítógépről (ez esetben a RAM-ról) kapott információk listázása.

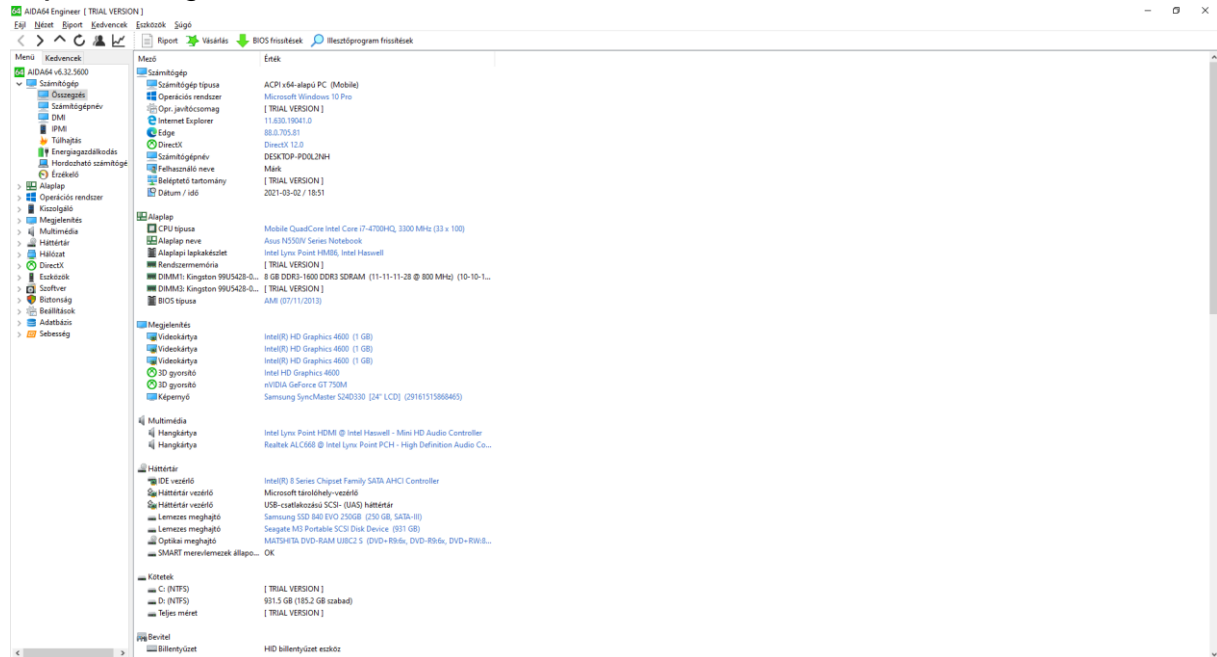


3. A számítógépet elemző szoftverek futtatása:

a. AIDA64:

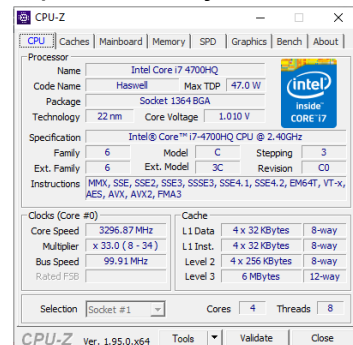
A számítógépről ad egy átfogó leírást, valamint különböző parancsok

hajthatók végre vele.



b. CPU-Z:

A processzor jellemzőinek részletes leírása.



c. GPU-Z:

A videokártya adatainak átfogó bemutatása.

