

Operációs rendszerek BSc

2. gyak.

2021. 02. 17.

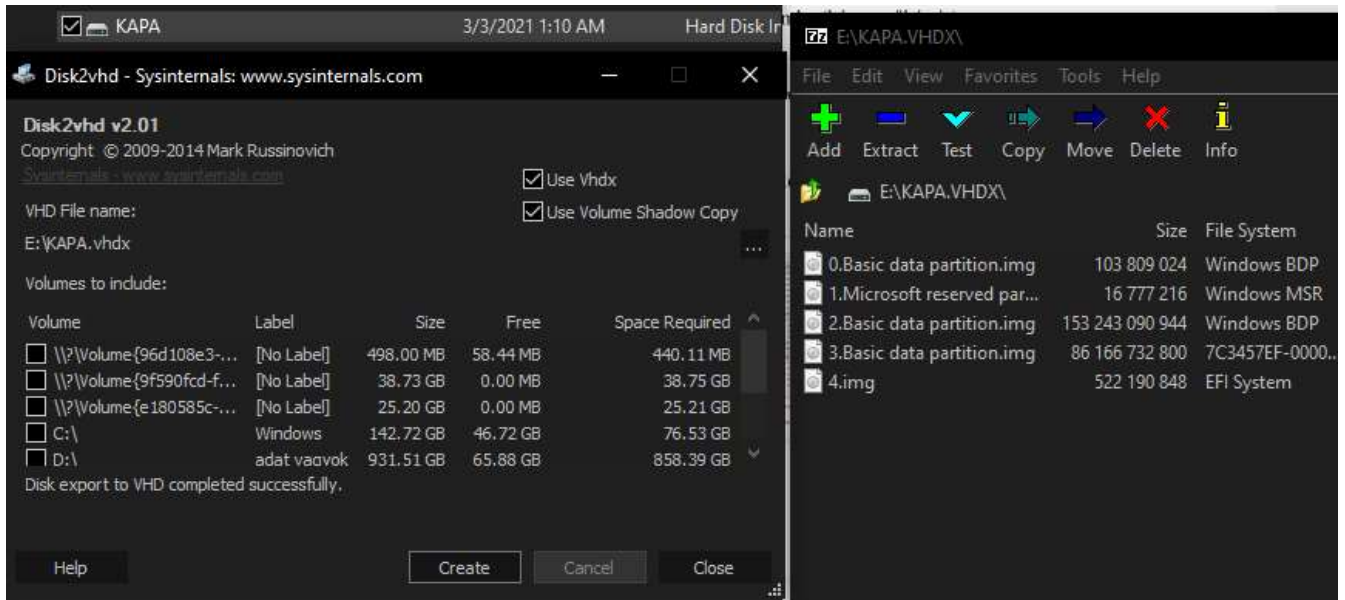
Készítette:

Simonyák János Bsc
Üzemmérnök-informatikus
MZ727W

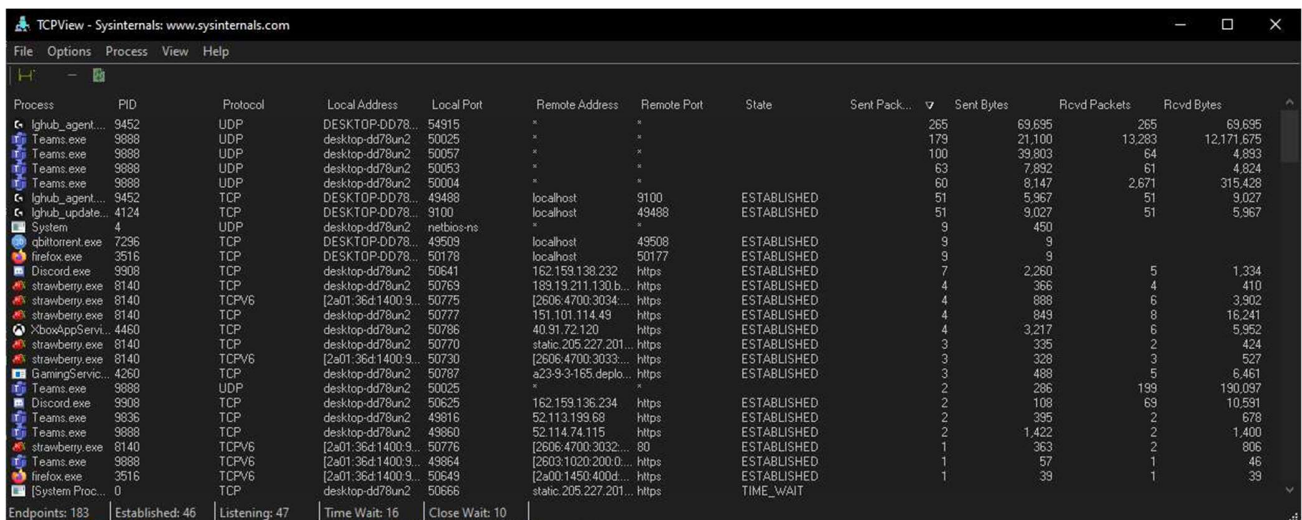
Miskolc, 2021

2.) feladat: Sysinternals segédprogramok

- a) Disk2vhd: Merevlemezek másolatainak készítése, .vhdx/.vhd fájlalba csomagolva, pl. virtuális számítógéphez.



- b) TCPView: milyen programok milyen címre, milyen porton csatlakoznak. Küldött, kapott bájtok és csomagok.



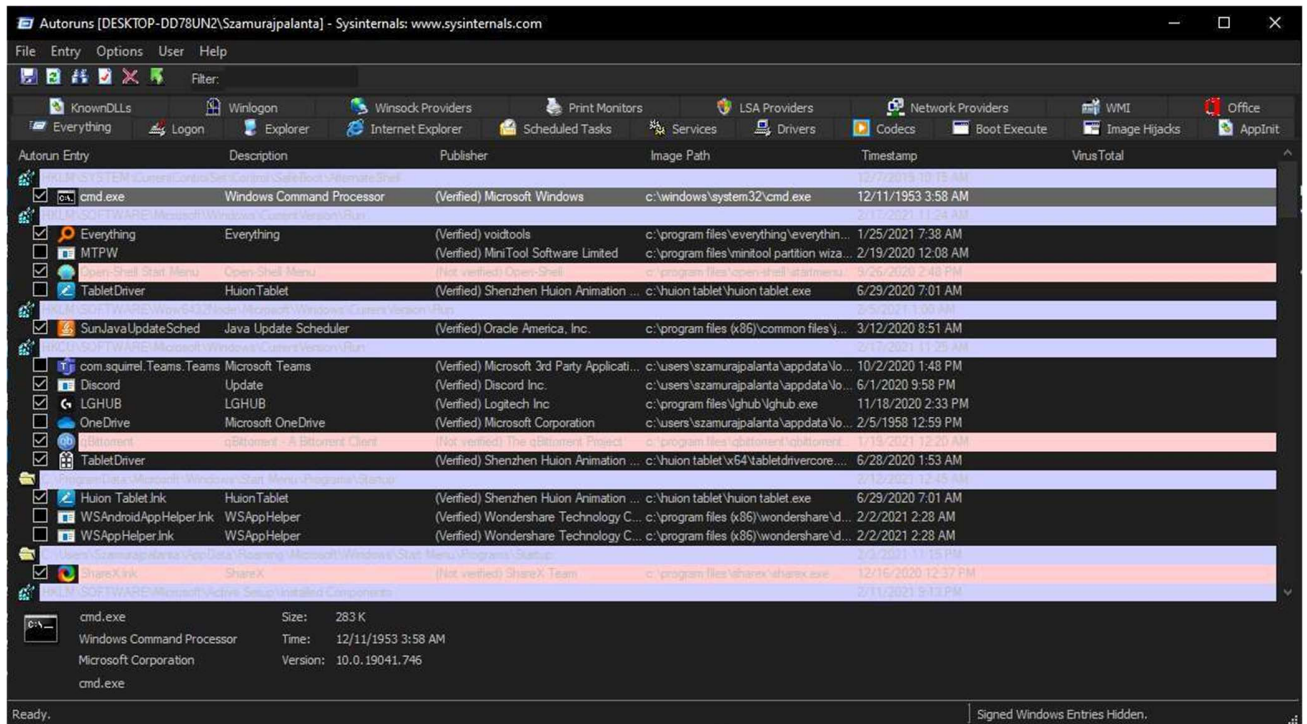
- c) Process Explorer: Szintekre vannak osztva a folyamatok attól függően, hogy melyik folyamat alfolyamata egy program.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
lghub.exe		33,100 K	44,900 K	9640	LGHUB	Logitech, Inc.
lghub.exe		10,460 K	30,688 K	10000	LGHUB	Logitech, Inc.
qbittorrent.exe	0.48	23,172 K	19,060 K	7296	qBittorrent - A BitTorrent Client	The qBittorrent Project
TabletDriverCore.exe	0.05	12,440 K	11,028 K	1288		
XboxAppServices.exe		6,016 K	33,268 K	4460		
ShareX.exe	< 0.01	73,796 K	99,500 K	12088	ShareX	ShareX Team
Code.exe	0.57	42,456 K	79,264 K	10940	Visual Studio Code	Microsoft Corporation
Code.exe		9,388 K	21,396 K	1712	Visual Studio Code	Microsoft Corporation
Code.exe	0.05	365,668 K	104,736 K	10980	Visual Studio Code	Microsoft Corporation
Code.exe		12,092 K	35,464 K	11832	Visual Studio Code	Microsoft Corporation
Code.exe	< 0.01	40,008 K	71,832 K	6968	Visual Studio Code	Microsoft Corporation
Code.exe	0.03	78,296 K	88,744 K	7208	Visual Studio Code	Microsoft Corporation
CodeHelper.exe		11,032 K	15,284 K	4840	CodeHelper	Microsoft Corporation
conhost.exe	< 0.01	41,032 K	74,028 K	1780	Console Window Host	Microsoft Corporation
Code.exe		110,340 K	110,340 K	10520	Visual Studio Code	Microsoft Corporation
strawberry.exe	1.79	103,552 K	110,340 K	8140	Strawberry Music Player	Strawberry
strawberry-tagreader.exe		3,388 K	9,736 K	11528		
conhost.exe		6,320 K	5,372 K	5508	Console Window Host	Microsoft Corporation
strawberry-tagreader.exe		3,968 K	10,660 K	11124		
conhost.exe		6,348 K	5,372 K	6300	Console Window Host	Microsoft Corporation
swriter.exe		748 K	3,792 K	6292	LibreOffice Writer	The Document Foundation
soffice.exe		1,184 K	5,384 K	12720	LibreOffice	The Document Foundation
soffice.bin	0.02	739,840 K	356,268 K	6120	LibreOffice	The Document Foundation
thunderbird.exe		174,572 K	229,944 K	10440	Thunderbird	Mozilla Corporation
procexp64.exe	4.38	30,136 K	55,024 K	5172	Sysinternals Process Explorer	Sysinternals - www.sysinter...
updatechecker.exe		8,800 K	3,828 K	8444		
Discord.exe	< 0.01	35,148 K	59,896 K	600	Discord	Discord Inc.
Discord.exe		10,972 K	22,012 K	9476	Discord	Discord Inc.
Discord.exe		171,460 K	139,892 K	9724	Discord	Discord Inc.

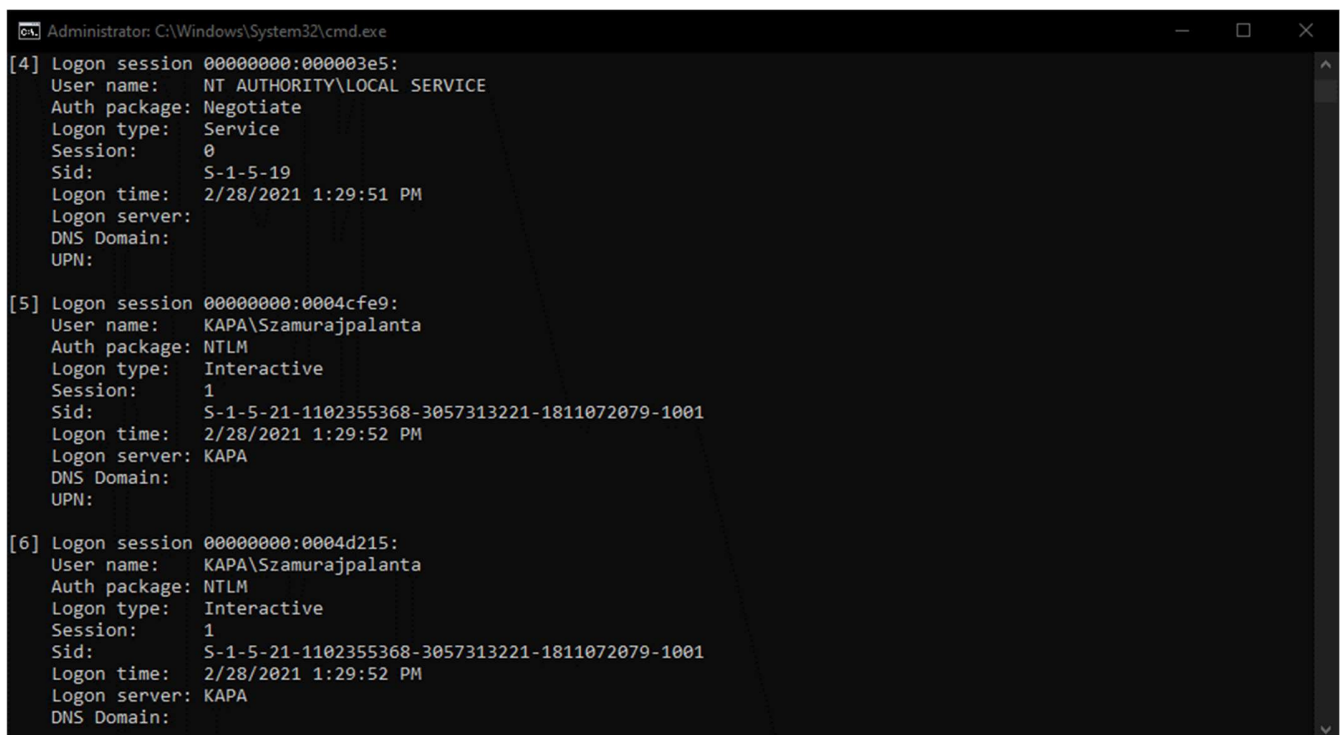
Process Monitor: Fájrendszer, registry monitorozása processzenként.

Time	Process Name	PID	Operation	Path	Result	Detail
1:22:5...	Sysmon64.exe	4204	ReadFile	C:\Windows\System32\crypt32.dll	SUCCESS	Offset: 1,215,488, Length: 4,096, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	svchost.exe	2552	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690,688, Length: 15,872, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	Sysmon64.exe	4204	ReadFile	C:\Windows\System32\wintrust.dll	SUCCESS	Offset: 305,664, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	svchost.exe	2552	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 678,400, Length: 12,288, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	MsMpEng.exe	4680	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14,254,080, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	Sysmon64.exe	4204	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 14,049,280, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	svchost.exe	2552	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 1,631,232, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	MsMpEng.exe	4680	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 644,096, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	Sysmon64.exe	4204	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 1,614,848, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	MsMpEng.exe	4680	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 5,083,136, Length: 4,096, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	MsMpEng.exe	4680	ReadFile	C:\Users\Szamuraipalanta\Downloads\...	NAME NOT FOUND	Desired Access: Read Data/List Directory, Read Attributes, Read Control, Synchronize, Disposition: Open, Options: Open Req...
1:22:5...	svchost.exe	2552	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 14,467,072, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	MsMpEng.exe	4680	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 1,598,464, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	svchost.exe	2552	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 627,712, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
1:22:5...	MsMpEng.exe	4680	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 5,070,848, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal

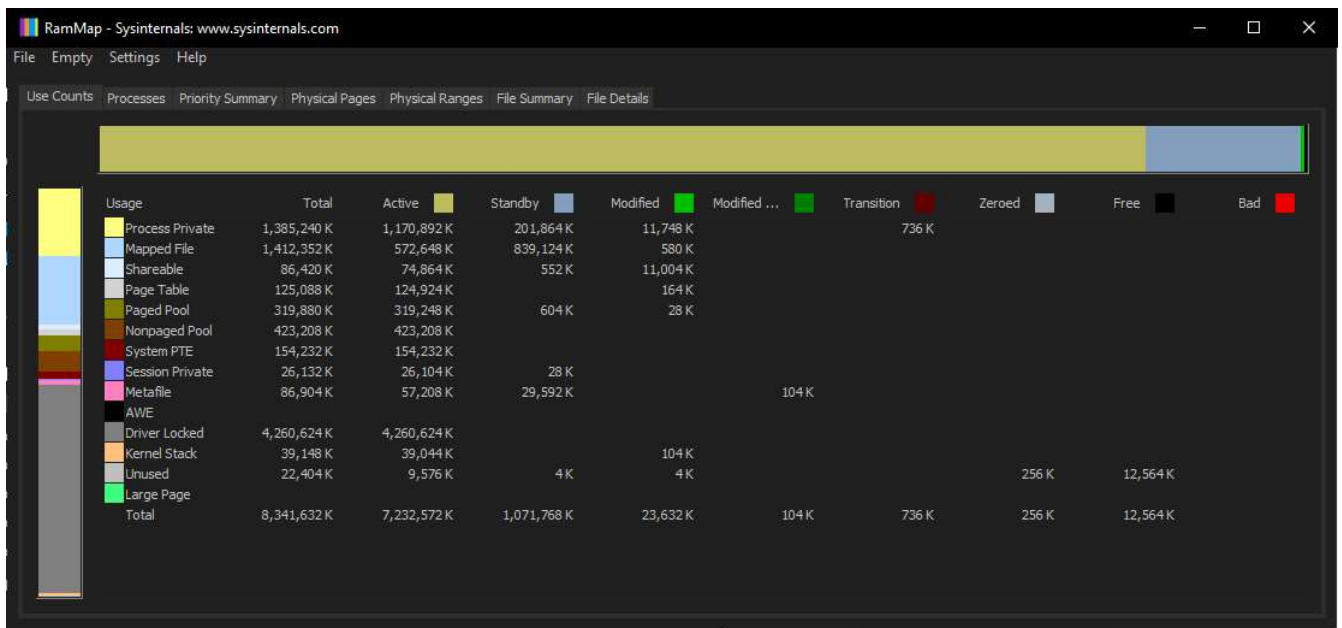
Autoruns: Az operációs rendszer indulása után elinduló programokat listázza.



d) LogonSessions: Bejelentkezések kiírása a parancssorba, szolgáltatások és felhasználók által is.



e) RAMMap: A számítógép memóriájának tartalmának térképszerű és listázott kiírása.



3.) feladat: AIDA64

Átfogó rendszerinformációs és stressztesztelő program.

