

Operációs rendszerek BSc

2. Gyak.

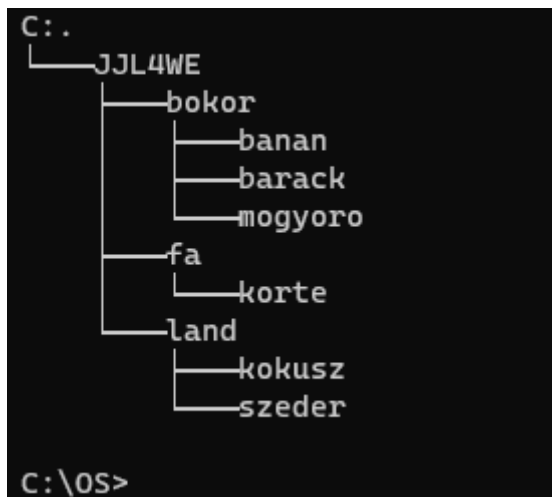
2022. 02. 14.

Készítette:

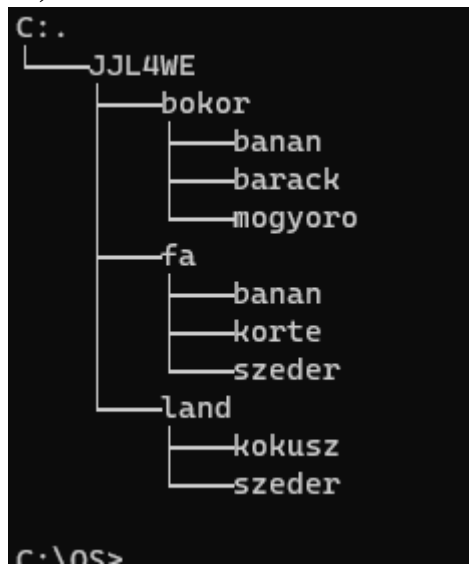
Hauer Attila Árpád Bsc
Mérnökinformatikus Szak
Neptunkód : JYL4WE

Miskolc, 2022

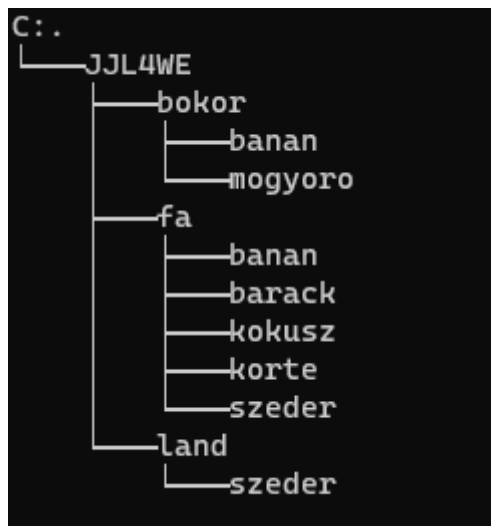
1. feladat – a)



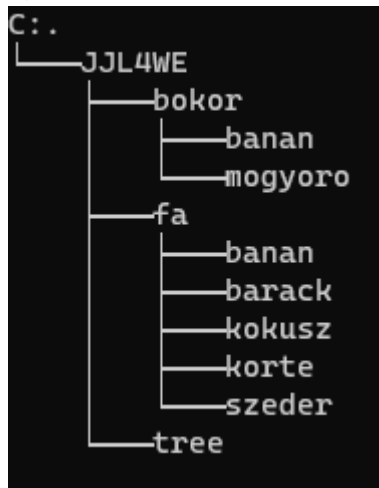
b)



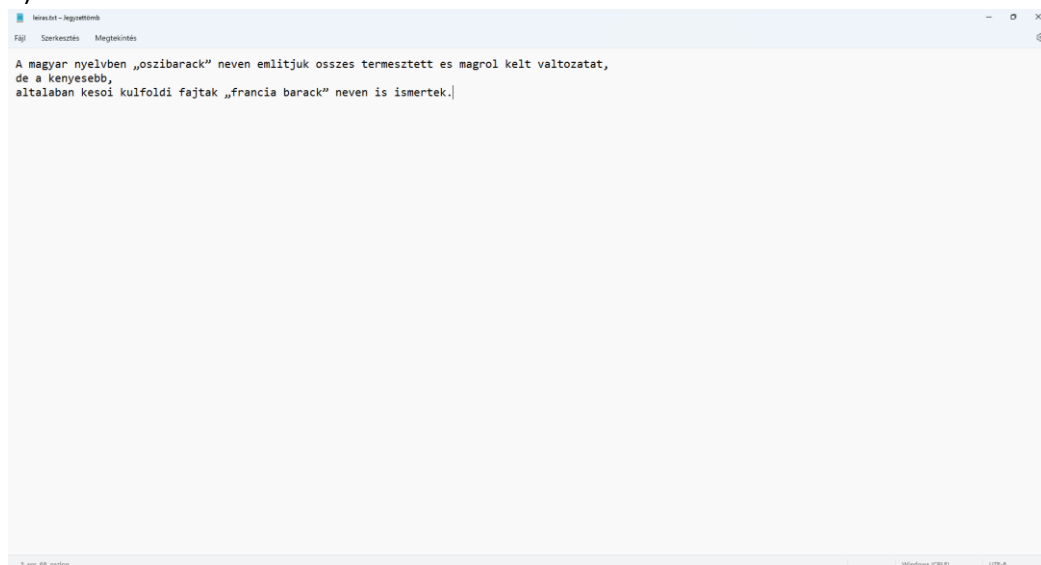
c)

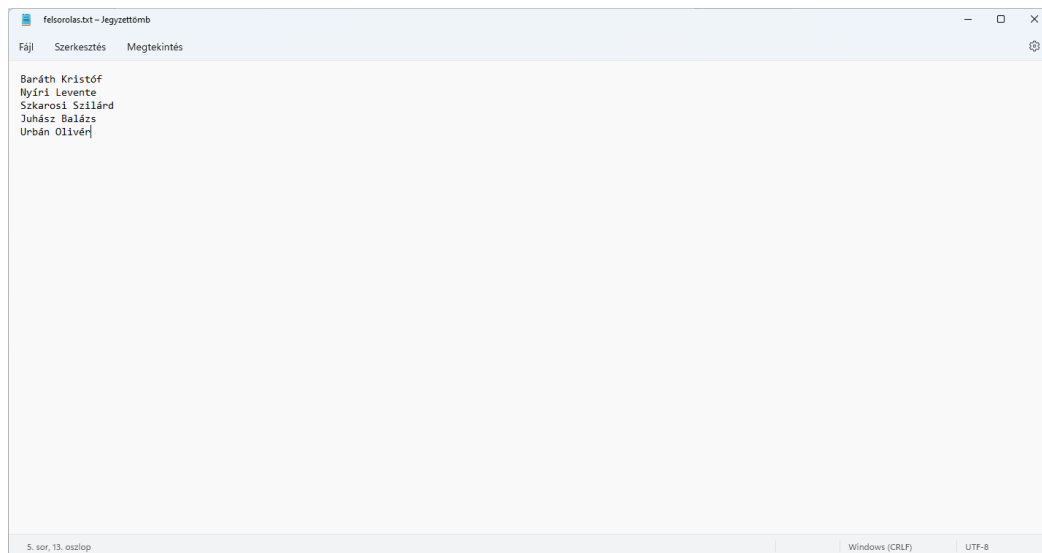


d)

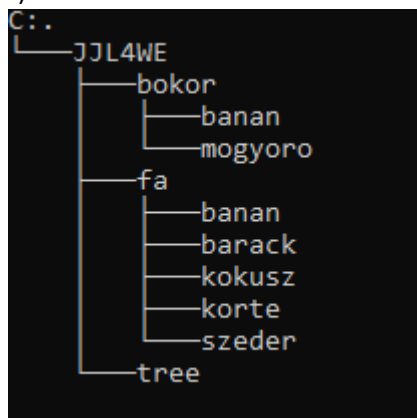


e)





f)



g)

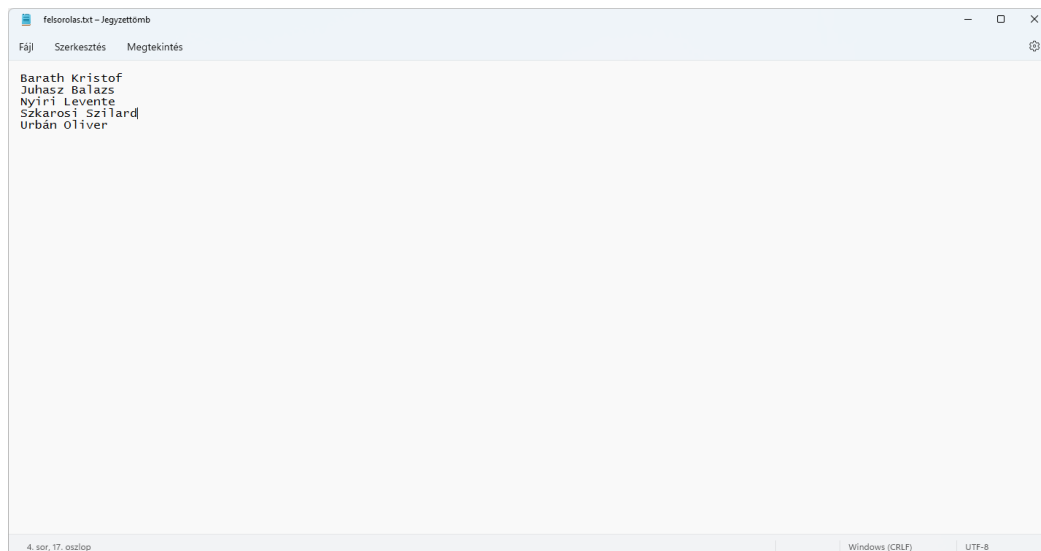
Nincs a feltételnek megfelelő mappa!!!

i)

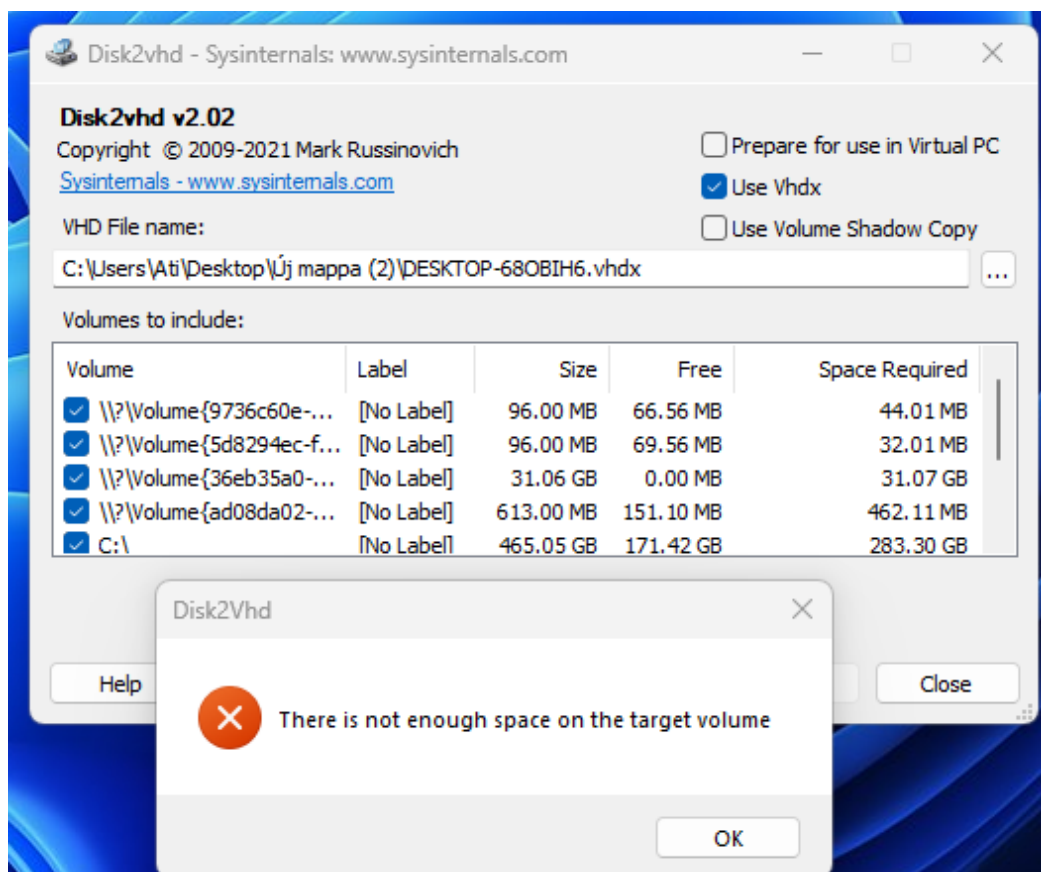
```
Directory of C:\OS\JLL4WE\tree
2022. 02. 20. 16:21 <DIR> .
2022. 02. 20. 16:21 <DIR> ..
2022. 02. 20. 16:41 77 felsorolas.txt.txt
                        77 bytes
                1 File(s)

Total Files Listed:
                2 File(s)        264 bytes
```

j)



2) a)



Wireshark - SystemTools www.systemtools.com													
File Edit View Process Connections Options Help													
Process Name	Process ID	Protocol	Status	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets	Sent Bytes	Recv Bytes
W:\System	1064	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022-02-26 10:17:15	tcp.sys				
W:\System	4	TCP	Listen	192.168.194.182	139	0.0.0.0	0	2022-02-26 10:17:12	System				
W:\System	4	TCP	Listen	192.168.0.2	139	0.0.0.0	0	2022-02-26 10:17:12	System				
W:\OriginWebHelperService...	4480	TCP	Listen	127.0.0.1	8213	0.0.0.0	0	2022-02-26 10:17:18	Origin Web Helper Service				
W:\System	9440	TCP	Listen	0.0.0.0	3540	0.0.0.0	0	2022-02-26 10:17:18	CDPVC				
W:\System	1040	TCP	Listen	127.0.0.1	8401	0.0.0.0	0	2022-02-26 10:17:13	Discord.exe				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	1320	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12110	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12119	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12120	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12121	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12122	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12123	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12124	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12125	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12126	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12127	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12128	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12129	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12130	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12131	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12132	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12133	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12134	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12135	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12136	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12137	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12138	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				
W:\AvastSvc.exe	3444	TCP	Listen	127.0.0.1	12139	0.0.0.0	0	2022-02-26 10:17:26	avast! Antivirus				

Time	Process Name	PID	Operation	Path	Result	Detail
17:20	svchost.exe	1760	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 651 264, Le...
17:20	svchost.exe	1760	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
17:20	svchost.exe	1760	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124, Length...
17:20	svchost.exe	1760	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Deared Access: R...
17:20	svchost.exe	1760	RegOpenKey	HKU\S-1-5-18	REPARSE	Deared Access: M...
17:20	svchost.exe	1760	RegQueryValue	HKU\DEFAULT	SUCCESS	Deared Access: M...
17:20	svchost.exe	1760	RegOpenKey	HKU\DEFAULT\Software\Policies\Mic...	NAME NOT FOUND	Deared Access: R...
17:20	svchost.exe	1760	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop...	SUCCESS	Deared Access: R...
17:20	svchost.exe	1760	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop...	SUCCESS	Offset: 124, Length...
17:20	svchost.exe	1760	RegOpenKey	HKU\DEFAULT	SUCCESS	
17:20	svchost.exe	1760	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Deared Access: R...
17:20	svchost.exe	1760	RegOpenKey	HKU\S-1-5-18	REPARSE	Deared Access: M...
17:20	svchost.exe	1760	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
17:20	svchost.exe	1760	RegOpenKey	HKU\DEFAULT\Software\Policies\Mic...	NAME NOT FOUND	Deared Access: R...
17:20	svchost.exe	1760	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop...	NAME NOT FOUND	Deared Access: R...
17:20	svchost.exe	1760	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124, Length...
17:20	svchost.exe	1760	RegOpenKey	HKU\DEFAULT	SUCCESS	
17:20	lsass.exe	1004	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 527 808...
17:20	lsass.exe	1004	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 511 424...
17:20	lsass.exe	1004	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 503 232...
17:20	lsass.exe	1004	QueryNameInfo	C:\Users\A\h\Desktop\Új mappa (2).Pro...	SUCCESS	Name: \Users\A\h\...
17:20	lsass.exe	1004	QueryNameInfo	C:\Users\A\h\Desktop\Új mappa (2).Pro...	SUCCESS	Name: \Users\A\h\...
17:20	svchost.exe	1760	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
17:20	svchost.exe	1760	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124, Length...
17:20	Explorer.EXE	9512	ReadFile	C:\Windows\System32\ShCore.dll	SUCCESS	Offset: 827 392, Le...
17:20	Explorer.EXE	9512	ReadFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
17:20	svchost.exe	1760	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124, Length...
17:20	Explorer.EXE	9512	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2 290 176...
17:20	Explorer.EXE	9512	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
17:20	svchost.exe	1760	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Deared Access: R...
17:20	Explorer.EXE	9512	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
17:20	svchost.exe	1760	RegOpenKey	HKCU\Software\Classes	SUCCESS	Deared Access: M...
17:20	svchost.exe	1760	RegOpenKey	HKU\DEFAULT	SUCCESS	Deared Access: M...
17:20	Explorer.EXE	9512	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Deared Access: R...
17:20	svchost.exe	1760	RegOpenKey	HKU\DEFAULT\Software\Policies\Mic...	NAME NOT FOUND	Deared Access: R...
17:20	Explorer.EXE	9512	RegOpenKey	HKCR\Applications\Promon64.exe	NAME NOT FOUND	Deared Access: R...
17:20	svchost.exe	1760	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop...	SUCCESS	Deared Access: R...

Showing 139 890 of 252 341 events (55%)

Backed by virtual memory

autorun:

Autoruns Entry	Description	Publisher	Image Path	Timestamp
Internet Explorer				
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				Sat Feb 19 18:06:27 2022
IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\98.0.1108.56\BHO...	Thu Feb 17 08:23:55 2022
Skype for Business Browser Helper	Skype for Business	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\OCHelper.dll	Wed Feb 2 12:27:29 2022
HKLM\Software\Microsoft\Internet Explorer\Extensions				Sat Feb 19 18:09:25 2022
Lync Click to Call	Skype for Business	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\OCHelper.dll	Wed Feb 2 12:27:29 2022
OneNote Linked Notes	Microsoft OneNote Internet Explorer Add...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\ONBtttrELinkedNotes...	Wed Feb 2 12:27:48 2022
Send to OneNote	Microsoft OneNote Internet Explorer Add...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\ONBtttrEL.dll	Wed Feb 2 12:27:48 2022
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				Sat Feb 19 18:07:43 2022
IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\98.0.1108.56\BHO...	Thu Feb 17 08:22:41 2022
Skype for Business Browser Helper	Skype for Business	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VF3\ProgramFilesX86\Microsoft...	Sun Oct 31 11:30:33 2021
Java(TM) Plug-In SSV Helper	Java(TM) Platform SE binary	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Java\jre1.8.0_291\bin\jpsv.dll	Thu May 27 14:43:47 2021
Java(TM) Plug-In 2 SSV Helper	Java(TM) Platform SE binary	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Java\jre1.8.0_291\bin\jps2sv.dll	Thu May 27 14:43:47 2021
HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Extensions				Sat Feb 19 18:07:38 2022
Lync Click to Call	Skype for Business	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VF3\ProgramFilesX86\Microsoft...	Sun Oct 31 11:30:33 2021
OneNote Linked Notes	Microsoft OneNote Internet Explorer Add...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VF3\ProgramFilesX86\Microsoft...	Wed Feb 2 12:32:30 2022
Send to OneNote	Microsoft OneNote Internet Explorer Add...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\VF3\ProgramFilesX86\Microsoft...	Wed Feb 2 12:32:29 2022
Boot Execute				
Image Hijacks				
HKLM\SOFTWARE\Classes\HtmFile\Shell\Open\Command(Default)	Internet Explorer	(Verified) Microsoft Corporation	C:\Program Files\Internet Explorer\iexplore.exe	Sat Feb 19 17:52:11 2022
C:\Program Files\Internet Explorer\iexplore.exe				Fri Feb 11 00:00:00 2022
Appinit				

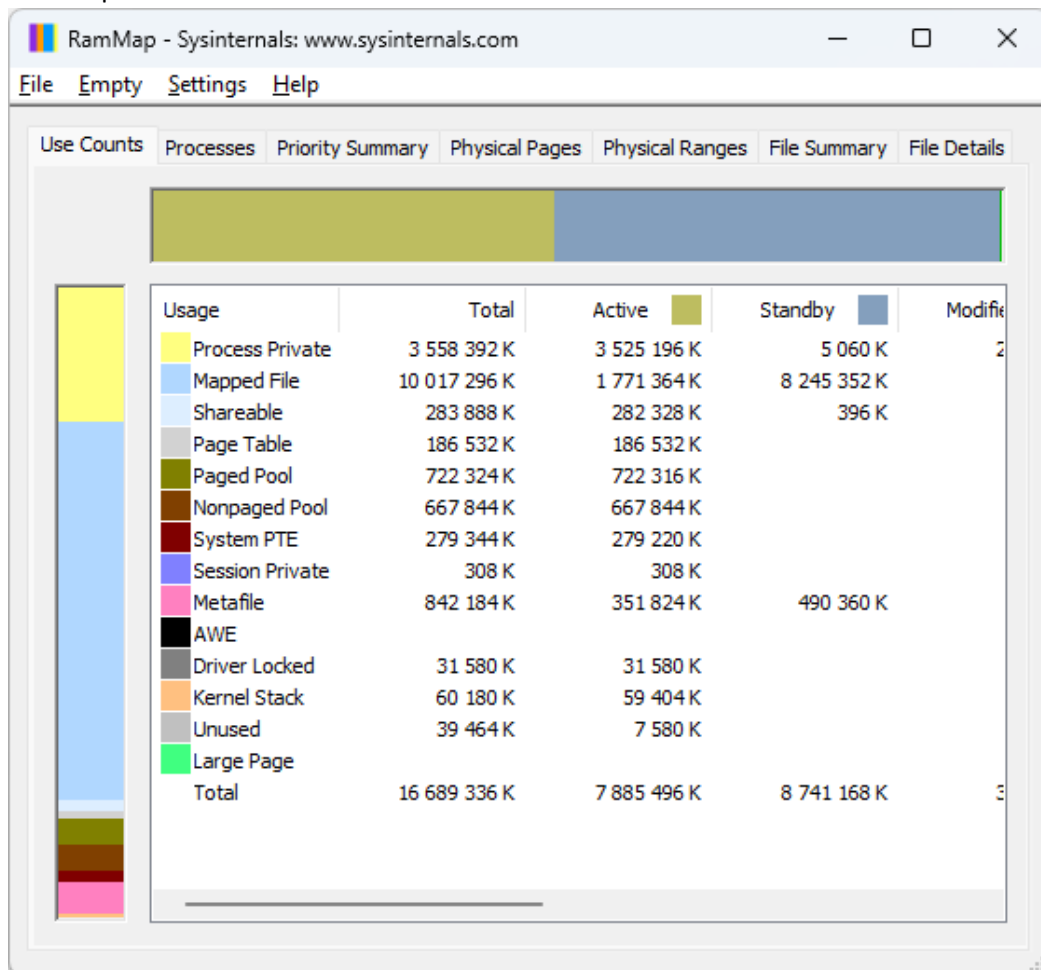
d)

C:\Users\A\h\Desktop\Új mappa
Termination behavior can be configured in advanced profile settings. Don't show again
<p>LgongSessions v1.41 - Lists logon session information</p> <p>Copyright (C) 2004-2020 Mark Russinovich</p> <p>Sysinternals - www.sysinternals.com</p> <p>Initialization error:</p> <p>Make sure that you are an administrator and run from an administrative command prompt.</p> <p>[Process exited with code 1 (0x00000001)]</p>

amúgy meg ha elindítom akkor eltűnik(rendszergazd. módba)

e)

ram map:



3)

