

Operációs rendszerek BSc

2.Gyak

2022.02.15

Készítette:

Kormos Balázs

Mérnökinformatikus

YE6BLB

Miskolc, 2022

1.feladat:

a) Hozza létre a következő mappa szerkezetet!

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Minden jog fenntartva.
C:\Users\User>cd..
C:\Users>cd..
C:\>md YE6BLB
C:\>cd YE6BLB
C:\YE6BLB>md bokor
C:\YE6BLB>cd bokor
C:\YE6BLB\bokor>md banan
C:\YE6BLB\bokor>md mogyoro
C:\YE6BLB\bokor>md barack
C:\YE6BLB\bokor>cd..
C:\YE6BLB>md fa
C:\YE6BLB>cd fa
C:\YE6BLB\fa>md korte
C:\YE6BLB\fa>cd..
C:\YE6BLB>md land
C:\YE6BLB>cd land
C:\YE6BLB\land>md szeder
C:\YE6BLB\land>md kokusz
C:\YE6BLB\land>
```

b) Készítsen másolatot:

- a neptunkod/ land/szeder katalógusról a neptunkod/fa katalógusba
- a neptunkod /bokor/banan katalógusról a neptunkod /fa katalógusba

```
C:\YE6BLB>Xcopy /E C:\YE6BLB\land\szeder C:\YE6BLB\fa
0 File(s) copied
C:\YE6BLB>Xcopy /E C:\YE6BLB\bokor\banan C:\YE6BLB\fa
0 File(s) copied
C:\YE6BLB>
```

c) Végezze el a következő áthelyezéseket:

- a neptunkod /bokor/barack katalógust helyezze át a neptunkod /fa katalógusba
- a neptunkod /land /kokusz katalógust helyezze át a neptunkod/fa katalógusba

```
C:\YE6BLB>move \YE6BLB\bokor\barack \YE6BLB\fa\  
1 dir(s) moved.  
C:\YE6BLB>move \YE6BLB\land\kokusz \YE6BLB\fa\  
1 dir(s) moved.  
C:\YE6BLB>
```

d) Törölje a neptunkod/land katalógust a teljes tartalmával. Hozza létre a következő szöveges állományokat:

- neptunkod/bokor/banan/ leiras.txt
- neptunkod/tree/felsorolas.txt

```
C:\>rmdir /s YE6BLB\land  
YE6BLB\land, Are you sure (Y/N)? y  
C:\>cd YE6BLB  
C:\YE6BLB>cd bokor  
C:\YE6BLB\bokor>cd banan  
C:\YE6BLB\bokor\banan>type nul > leiras.txt  
C:\YE6BLB\bokor\banan>cd..  
C:\YE6BLB\bokor>cd..  
C:\YE6BLB>cd fa  
C:\YE6BLB\fa>type nul > felsorolas.txt  
C:\YE6BLB\fa>
```

e) A leiras.txt szöveges állományba írjon 3 sort a barackról.

A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

```

C:\YE6BLB\bokor\banan>notepad leiras
C:\YE6BLB\bokor\banan>type leiras.txt
a barack finom mint
etel es mint
ital
C:\YE6BLB\bokor\banan>cd..
C:\YE6BLB\bokor>cd..
C:\YE6BLB>cd fa
C:\YE6BLB\fa>notepad felsorolas
C:\YE6BLB\fa>type felsorolas.txt
Zoltan
Patrik
Bence
Alen
Roland
C:\YE6BLB\fa>

```

f) Listázza a neptunkod mappa tartalmát úgy, hogy megjelenjen az almappák tartalma is.

```

C:\YE6BLB>tree \YE6BLB /f
Folder PATH listing
Volume serial number is E200-3DDB
C:\YE6BLB
├── bokor
│   ├── banan
│   │   └── leiras.txt
│   └── mogyoro
└── fa
    ├── felsorolas.txt
    ├── barack
    ├── kokusz
    └── korte
C:\YE6BLB>

```

g) Térjen vissza a gyökérmappába és keresse meg az összes olyan file-t, amelyek nevének második betűje e.

```

C:\YE6BLB>dir /s *.*
Volume in drive C has no label.
Volume Serial Number is E200-3DDB

Directory of C:\YE6BLB\bokor\banan
2022.02.21.  23:17                39 leiras.txt
               1 File(s)              39 bytes

Directory of C:\YE6BLB\fa
2022.02.21.  23:21                35 felsorolas.txt
2022.02.21.  09:19                <DIR>
               1 File(s)              35 bytes

Total Files Listed:
                2 File(s)              74 bytes
                1 Dir(s)  34 817 896 448 bytes free

C:\YE6BLB>

```

h) Tegye mindenki számára olvashatóvá a felsorolas.txt file-t

```

C:\YE6BLB>cd fa
C:\YE6BLB\fa>attrib
A                C:\YE6BLB\fa\felsorolas.txt
C:\YE6BLB\fa>attrib +r felsorolas.txt
C:\YE6BLB\fa>attrib
A      R        C:\YE6BLB\fa\felsorolas.txt
C:\YE6BLB\fa>

```

i) Jelenítse meg, hogy mennyi helyet foglal a merevlemezen a neptunkod mappa az al-mappáival együtt.

```

C:\YE6BLB>dir /s
Volume in drive C has no label.
Volume Serial Number is E200-3DDB

Directory of C:\YE6BLB

2022.02.21.  23:01    <DIR>        .
2022.02.21.  23:01    <DIR>        ..
2022.02.21.  12:54    <DIR>        bokor
2022.02.21.  23:06    <DIR>        fa
                0 File(s)                0 bytes

Directory of C:\YE6BLB\bokor

2022.02.21.  12:54    <DIR>        .
2022.02.21.  12:54    <DIR>        ..
2022.02.21.  23:05    <DIR>        banan
2022.02.21.  09:19    <DIR>        mogyoro
                0 File(s)                0 bytes

Directory of C:\YE6BLB\bokor\banan

2022.02.21.  23:05    <DIR>        .
2022.02.21.  23:05    <DIR>        ..
2022.02.21.  23:17                39 leiras.txt
                1 File(s)                39 bytes

Directory of C:\YE6BLB\bokor\mogyoro

2022.02.21.  09:19    <DIR>        .
2022.02.21.  09:19    <DIR>        ..
                0 File(s)                0 bytes

Directory of C:\YE6BLB\fa

2022.02.21.  23:06    <DIR>        .
2022.02.21.  23:06    <DIR>        ..
2022.02.21.  09:19    <DIR>        barack
2022.02.21.  23:21                35 felsorolas.txt
2022.02.21.  09:19    <DIR>        kokusz
2022.02.21.  09:19    <DIR>        korte
                1 File(s)                35 bytes

Directory of C:\YE6BLB\fa\barack

2022.02.21.  09:19    <DIR>        .
2022.02.21.  09:19    <DIR>        ..
                0 File(s)                0 bytes

Directory of C:\YE6BLB\fa\kokusz

2022.02.21.  09:19    <DIR>        .
2022.02.21.  09:19    <DIR>        ..
                0 File(s)                0 bytes

Directory of C:\YE6BLB\fa\korte

2022.02.21.  09:19    <DIR>        .
2022.02.21.  09:19    <DIR>        ..
                0 File(s)                0 bytes

Total Files Listed:
                2 File(s)                74 bytes
                23 Dir(s)  34 802 667 520 bytes free

C:\YE6BLB>

```

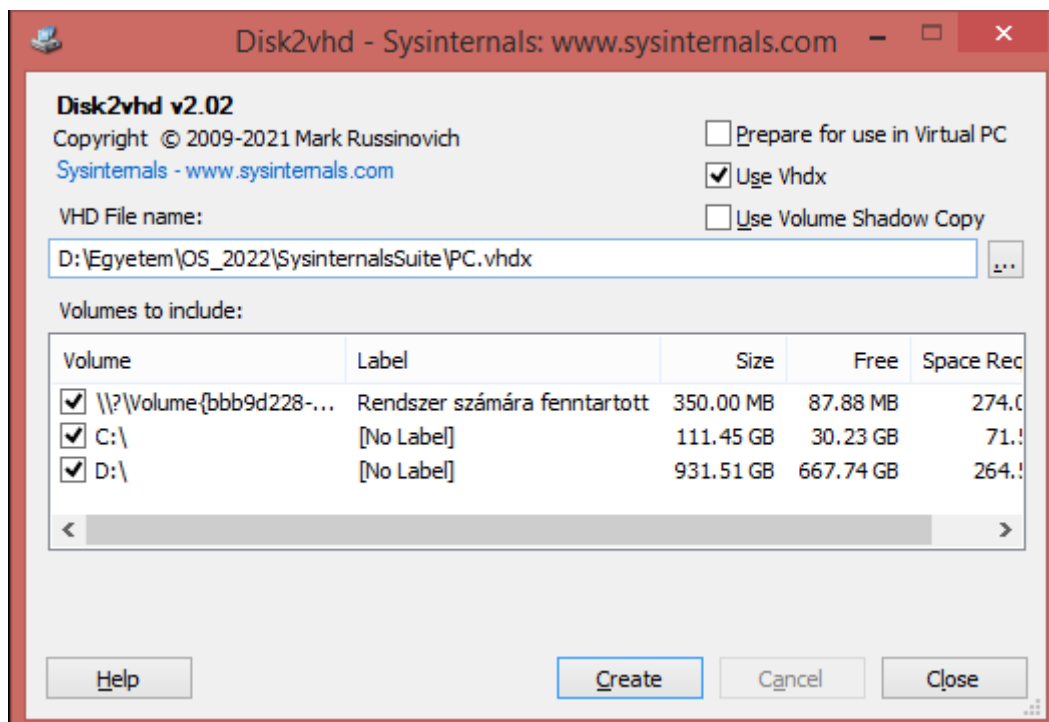
j) Rendezze ABC-szerint a felsorolas.txt file tartalmát.

```
C:\YE6BLB>cd fa
C:\YE6BLB\fa>sort felsorolas.txt
Alen
Bence
Patrik
Roland
Zoltan
C:\YE6BLB\fa>
```

2. feladat:

a)

A Disk2vhd egy olyan segédprogram, amely létrehozza a fizikai lemezek VHD-verzióit (Virtuális merevlemez – A Microsoft virtuálisgép-lemezformátuma) a Microsoft Virtual PC-n vagy Microsoft Hyper-V virtuális gépeken való használatra



b)

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.

TCPView - Sysinternals www.sysinternals.com													
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets	Sent Bytes	Recv Bytes
TeamViewer_Service...	3104	UDP		192.168.0.115	5353 *			2022.02.26, 10:13:28	TeamViewer				
nvcontainer.exe	2520	UDP		192.168.0.115	5353 *			2022.02.27, 10:25:59	nvcontainer.exe				
TeamViewer_Service...	3104	UDP		192.168.56.1	5353 *			2022.02.26, 10:13:28	TeamViewer				
nvcontainer.exe	2520	UDP		192.168.56.1	5353 *			2022.02.27, 10:25:59	nvcontainer.exe				
nvsvchost.exe	1268	UDP		0.0.0.0	5355 *			2022.02.27, 13:55:54	Dnscache				
NVIDIA Web Helper.exe	4636	UDP		127.0.0.1	10020 *			2022.02.27, 10:25:59	NVIDIA Web Helper.exe				
nvcontainer.exe	96	UDP		127.0.0.1	19021 *			2022.02.27, 10:26:19	nvcontainer.exe				
DiscSoftBusServiceL...	9596	UDP		0.0.0.0	43769 *			2022.02.26, 10:13:38	DiscSoftBusServiceL.exe				
dashHost.exe	2192	UDP		0.0.0.0	49643 *			2022.02.27, 10:25:57	dashHost.exe				
AvastSvc.exe	1372	UDP		127.0.0.1	50590 *			2022.02.26, 10:25:07	avast Antivirus				
AvastSvc.exe	1372	UDP		0.0.0.0	50592 *			2022.02.26, 10:25:07	avast Antivirus				
nvsvchost.exe	2980	UDP		0.0.0.0	54925 *			2022.02.26, 10:13:15	stacuc				
spoolsv.exe	1616	UDP		0.0.0.0	57460 *			2022.02.26, 10:13:25	Spooler				
nvsvchost.exe	3948	UDP		0.0.0.0	57461 *			2022.02.26, 10:13:25	FDResPub				
nvcontainer.exe	8536	UDP		127.0.0.1	60032 *			2022.02.27, 10:25:59	nvcontainer.exe				
nvcontainer.exe	2520	UDP		0.0.0.0	60542 *			2022.02.26, 10:13:41	nvcontainer.exe				
nvsvchost.exe	3948	UDP		192.168.0.115	61683 *			2022.02.27, 10:25:57	SSDPsrv				
nvsvchost.exe	3948	UDP		127.0.0.1	61684 *			2022.02.27, 10:25:57	SSDPsrv				
nvsvchost.exe	1064	UDP		0.0.0.0	61685 *			2022.02.27, 10:25:57	EventSystem				
TeamViewer_Service...	3104	UDP		0.0.0.0	62454 *			2022.02.26, 10:13:25	TeamViewer				
chrome.exe	820	UDP		0.0.0.0	5353 *			2022.02.27, 10:32:36	chrome.exe				
chrome.exe	524	UDP		0.0.0.0	5353 *			2022.02.27, 10:32:36	chrome.exe				
LCore.exe	6800	UDP		0.0.0.0	54915 *			2022.02.27, 10:26:08	LCore.exe				
nvsvchost.exe	318	UDPv6		:::ffff::1999:aa13::548	548 *			2022.02.27, 10:13:37	Dhcp				
nvsvchost.exe	576	UDPv6		:::ffff::7539:1999:aa13::548	548 *			2022.02.27, 10:13:37	Dhcp				
nvsvchost.exe	3948	UDPv6		:::	1900 *			2022.02.27, 10:25:57	SSDPsrv				
nvsvchost.exe	3948	UDPv6		:::ffff::7539:1999:aa13::548	1900 *			2022.02.27, 10:25:57	SSDPsrv				
nvsvchost.exe	3948	UDPv6		:::ffff::7539:1999:aa13::548	1900 *			2022.02.27, 10:25:57	SSDPsrv				
nvsvchost.exe	1064	UDPv6		:::	1702 *			2022.02.27, 10:25:57	EventSystem				
nvsvchost.exe	1064	UDPv6		:::	1702 *			2022.02.27, 10:25:57	EventSystem				
nvsvchost.exe	3948	UDPv6		:::	1702 *			2022.02.27, 10:25:57	FDResPub				
nvsvchost.exe	2192	UDPv6		:::	1702 *			2022.02.27, 10:25:57	dashHost.exe				
nvsvchost.exe	3948	UDPv6		:::	1702 *			2022.02.27, 10:25:57	FDResPub				
nvsvchost.exe	2192	UDPv6		:::	1702 *			2022.02.27, 10:25:57	dashHost.exe				
chrome.exe	820	UDPv6		:::	5353 *			2022.02.27, 10:32:36	chrome.exe				
chrome.exe	524	UDPv6		:::	5353 *			2022.02.27, 10:32:36	chrome.exe				
nvcontainer.exe	2520	UDPv6		:::	5353 *			2022.02.27, 10:25:59	nvcontainer.exe				
TeamViewer_Service...	3104	UDPv6		:::	5353 *			2022.02.26, 10:13:28	TeamViewer				
nvsvchost.exe	1268	UDPv6		:::	5355 *			2022.02.27, 13:55:54	Dnscache				
dashHost.exe	2192	UDPv6		:::	49643 *			2022.02.27, 10:25:57	dashHost.exe				
LCore.exe	6800	UDPv6		:::	54915 *			2022.02.27, 10:26:08	LCore.exe				
nvsvchost.exe	3948	UDPv6		:::	57462 *			2022.02.26, 10:13:25	FDResPub				
nvcontainer.exe	2520	UDPv6		:::	60543 *			2022.02.26, 10:13:41	nvcontainer.exe				
nvsvchost.exe	3948	UDPv6		:::ffff:b0f4bbd4:55b6960	61681 *			2022.02.27, 10:25:57	SSDPsrv				
nvsvchost.exe	3948	UDPv6		:::	61682 *			2022.02.27, 10:25:57	SSDPsrv				
nvsvchost.exe	1064	UDPv6		:::	61686 *			2022.02.27, 10:25:57	EventSystem				
TeamViewer_Service...	3104	UDPv6		:::	62455 *			2022.02.26, 10:13:25	TeamViewer				

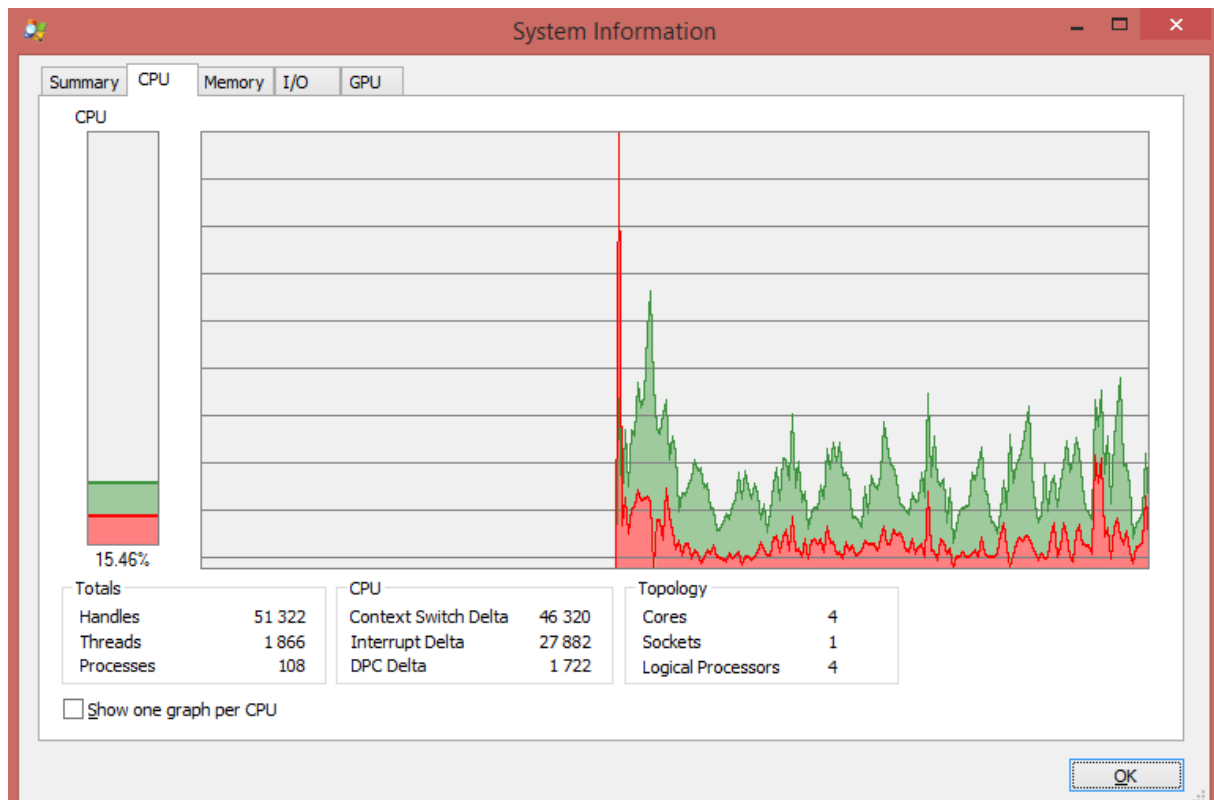
c)

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

A *Folyamatkezelő* megjelenítése két ablakból áll. A felső ablakban mindig megjelenik a jelenleg aktív folyamatok listája, beleértve a saját fiókjaik nevét, míg az alsó ablakban megjelenő információk a Folyamatkezelő módtól függnak: ha leíró módban van, a felső ablakban kiválasztott folyamat leírói jelennek meg; Ha a *Folyamatkezelő* DLL módban van, látni fogja a folyamat által betöltött DLL-eket és memória leképezett fájlokat.

Process Explorer - Sysinternals: www.sysinternals.com [Pc\User]						
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	80.83	0 K	4 K	0		
System	0.77	764 K	1 724 K	4		
smss.exe	1.16	0 K	0 K	n/a	Hardware Interrupts and DPCs	
csrss.exe		280 K	540 K	368		
wininit.exe		2 232 K	3 164 K	584		
services.exe		956 K	2 680 K	656		
svchost.exe		4 288 K	5 728 K	708		
WmPrvSE.exe		5 484 K	8 936 K	844	Windows-szolgáltatások gaz...	Microsoft Corporation
unsecapp.exe	1.55	9 876 K	13 748 K	5004		
RuntimeBroker.exe		1 092 K	1 820 K	7224		
svchost.exe		2 352 K	7 984 K	7724	Runtime Broker	Microsoft Corporation
svchost.exe		5 096 K	7 656 K	888	Windows-szolgáltatások gaz...	Microsoft Corporation
NVIDIA.Container.exe		4 496 K	9 084 K	1000	NVIDIA Container	NVIDIA Corporation
NVIDIA.Container.exe	< 0.01	31 444 K	56 416 K	8664		
svchost.exe	< 0.01	25 436 K	27 412 K	576	Windows-szolgáltatások gaz...	Microsoft Corporation
audiodg.exe	< 0.01	9 208 K	12 916 K	11532		
wscntfy.exe		7 560 K	8 952 K	856	Avast remediation.exe	AVAST Software
svchost.exe	< 0.01	25 352 K	37 340 K	1040	Windows-szolgáltatások gaz...	Microsoft Corporation
taskhost.exe		16 176 K	19 276 K	3756		
taskhost.exe		4 452 K	11 796 K	12248	Gazdálkodási Windows-fela...	Microsoft Corporation
svchost.exe		14 060 K	19 032 K	1064	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		18 340 K	22 604 K	1132	Windows-szolgáltatások gaz...	Microsoft Corporation
dshost.exe		6 196 K	11 516 K	2192		
WUDFHost.exe		3 700 K	12 392 K	6336		
svchost.exe		12 752 K	16 952 K	1268	Windows-szolgáltatások gaz...	Microsoft Corporation
AvastSvc.exe	< 0.01	135 656 K	40 924 K	1372	Avast Service	AVAST Software
aswEngSvc.exe		32 772 K	84 548 K	384		
aswToolsSvc.exe	< 0.01	56 376 K	59 884 K	1432	Avast Antivirus	AVAST Software
spoolsv.exe	< 0.01	4 892 K	6 100 K	1616	Várólista-alkalmazás kezelője	Microsoft Corporation
svchost.exe		25 356 K	27 520 K	1640	Windows-szolgáltatások gaz...	Microsoft Corporation
amsvc.exe		996 K	1 148 K	2016	Adobe Acrobat Update Servi...	Adobe Inc.
AdskLicensingService.exe		6 708 K	5 656 K	2036	Autodesk Desktop Licensing...	Autodesk
atxComSvc.exe		7 088 K	6 564 K	1224		
horizon_client_service.exe		2 836 K	4 964 K	1748	VMware Horizon Generic Ser...	VMware, Inc.
svchost.exe		5 040 K	9 500 K	2148	Windows-szolgáltatások gaz...	Microsoft Corporation
FNPLicensingService.exe		2 088 K	2 592 K	2200	Activation Licensing Service	Flexera
ftscanngrhvx.exe	< 0.01	3 416 K	3 168 K	2324	Scanner Redirection manag...	
LogRegistryService.exe		1 048 K	1 732 K	2460	Logitech Surround Sound Se...	Logitech Inc.
servicehost.exe	< 0.01	15 224 K	21 304 K	2476	McAfee WebAdvisor(service)	McAfee, LLC
lshost.exe	0.39	13 504 K	39 584 K	7956	McAfee WebAdvisor(serie...	McAfee, LLC
nvcontainer.exe	< 0.01	12 312 K	22 784 K	2520	NVIDIA Container	NVIDIA Corporation
nvcontainer.exe	< 0.01	8 796 K	26 780 K	96	NVIDIA Container	NVIDIA Corporation
NVIDIA.Share...	< 0.01	88 856 K	62 972 K	6128	NVIDIA Share	NVIDIA Corporation
NVIDIA.Share...		115 024 K	44 416 K	8928	NVIDIA Share	NVIDIA Corporation
NVIDIA.Share...		65 892 K	84 436 K	7580	NVIDIA Share	NVIDIA Corporation
nvcontainer.exe		35 692 K	50 344 K	8536	NVIDIA Container	NVIDIA Corporation
nvshelper64.exe	< 0.01	3 436 K	12 012 K	6108		
sqlwriter.exe		1 604 K	1 892 K	2848	SQL Server VSS Writer - 64 Bit	Microsoft Corporation
svchost.exe	< 0.01	10 056 K	10 804 K	2980	Windows-szolgáltatások gaz...	Microsoft Corporation
TeamViewer_Service.exe	< 0.01	17 068 K	8 232 K	3104	TeamViewer	TeamViewer Germany Gm...
vmtoolsd-pwks.exe	< 0.01	3 464 K	3 008 K	3184	Serial Com Redirection Client...	VMware
vmware-usbarbitrator64.exe	< 0.01	2 260 K	2 912 K	3344	VMware USB Arbitration Ser...	VMware, Inc.
SearchIndexer.exe		27 120 K	24 764 K	6024	A Microsoft Windows Search...	Microsoft Corporation
svchost.exe		4 528 K	10 332 K	3948	Windows-szolgáltatások gaz...	Microsoft Corporation
aswidsagent.exe	< 0.01	46 172 K	56 884 K	5472	Avast Software Analyzer	AVAST Software
DiscSoftBusServiceLite.exe		3 748 K	6 380 K	9596	Disc Soft Bus Service Lite	Disc Soft Ltd
BrYNSvc.exe		3 988 K	6 104 K	10136	BrYNSvc	Brother Industries, Ltd.
fntlsrv.exe	< 0.01	2 776 K	4 932 K	5248	NetLink sessionsservice	

CPU Usage: 19.72% | Commit Charge: 53.31% | Processes: 108 | Physical Usage: 52.32%



Process Monitor:

A *Folyamatfigyelő* egy fejlett monitorozási eszköz Windows, amely valós idejű fájlrendszer-, beállításjegyzék- és folyamat-/száltevékenységet mutat be.

Kombinálja két örökölt Sysinternals segédprogram, a *Filemon* és a *Regmon* funkcióit, és számos fejlesztést tartalmaz, többek között gazdag és nem kipusztító szűrést, átfogó eseménytulajdonságokat, például munkamenet-azonosítókat és felhasználóneveket, megbízható folyamatinformációkat, teljes szálkészleteket az egyes műveletek integrált szimbólumtámogatásával, a fájlba történő egyidejű naplózást. Egyedi funkciókkal a Folyamatfigyelő a rendszer hibaelhárítási és kártevőkeresési eszközkészletének egyik alapvető segédprogramja lesz.

Time	Process Name	PID	Operation	Path	Result	Detail
14:46	Explorer.EXE	8472	ReadFile	C:\Windows\System32\hunkscache.dll	SUCCESS	Offset: 111 616, Le...
14:46	ServiceHost.exe	2476	ReadFile	C:\Program Files\McAfee\WebAdvisor\...	SUCCESS	Offset: 3 743 232, ...
14:46	svchost.exe	2520	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 947 200, Le...
14:46	Explorer.EXE	8472	ReadFile	C:\Windows\WinSxS\amd64_microsoft...	SUCCESS	Offset: 2 160 640, ...
14:46	aswidsagent.exe	5472	CreateFile	C:\Windows\System32\drivers\PROCMI...	NAME NOT FOUND	Desired Access: R...
14:46	svchost.exe	2520	ReadFile	C:\Program Files\NVIDIA Corporation\...	SUCCESS	Offset: 449 536, Le...
14:46	Explorer.EXE	8472	NotifyChangeDi...	C:\Windows\System32	SUCCESS	Filter: FILE_NOTIFY...
14:46	aswidsagent.exe	5472	CreateFile	C:\Windows\System32\drivers	SUCCESS	Desired Access: R...
14:46	aswidsagent.exe	5472	QueryBasicInfor...	C:\Windows\System32\drivers	SUCCESS	CreationTime: 201...
14:46	aswidsagent.exe	5472	CloseFile	C:\Windows\System32\drivers	SUCCESS	
14:46	aswidsagent.exe	5472	CreateFile	C:\	SUCCESS	Desired Access: R...
14:46	Explorer.EXE	8472	QueryStandardI...	C:\Users\User\AppData\Local\Microso...	SUCCESS	AllocationSize: 831...
14:46	aswidsagent.exe	5472	QueryDirectory	C:\WINDOWS	SUCCESS	FileInformationClas...
14:46	aswidsagent.exe	5472	CloseFile	C:\	SUCCESS	
14:46	aswidsagent.exe	5472	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
14:46	Explorer.EXE	8472	CreateFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Desired Access: R...
14:46	aswidsagent.exe	5472	QueryDirectory	C:\Windows\SYSTEM32	SUCCESS	FileInformationClas...
14:46	Explorer.EXE	8472	QueryBasicInfor...	C:\Program Files\Internet Explorer\expl...	SUCCESS	CreationTime: 201...
14:46	Explorer.EXE	8472	CloseFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	
14:46	aswidsagent.exe	5472	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
14:46	ServiceHost.exe	2476	ReadFile	C:\Program Files\McAfee\WebAdvisor\...	SUCCESS	Offset: 3 681 792, ...
14:46	aswidsagent.exe	5472	CreateFile	C:\Windows\System32	SUCCESS	Desired Access: R...
14:46	aswidsagent.exe	5472	QueryDirectory	C:\Windows\System32\DRIVERS	SUCCESS	FileInformationClas...
14:46	aswidsagent.exe	5472	CloseFile	C:\Windows\System32	SUCCESS	
14:46	Explorer.EXE	8472	CreateFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Desired Access: R...
14:46	Explorer.EXE	8472	QueryBasicInfor...	C:\Program Files\Internet Explorer\expl...	SUCCESS	CreationTime: 201...
14:46	Explorer.EXE	8472	CloseFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	
14:46	aswidsagent.exe	5472	CreateFile	C:\Windows\System32\drivers\PROCMI...	NAME NOT FOUND	Desired Access: R...
14:46	Explorer.EXE	8472	CreateFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Desired Access: R...
14:46	aswidsagent.exe	5472	CreateFile	C:\Windows\System32\drivers\PROCMI...	NAME NOT FOUND	Desired Access: R...
14:46	Explorer.EXE	8472	QueryBasicInfor...	C:\Program Files\Internet Explorer\expl...	SUCCESS	CreationTime: 201...
14:46	Explorer.EXE	8472	CloseFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	
14:46	aswidsagent.exe	5472	CreateFile	C:\Windows\WinSxS\FileMap\ISS_syst...	SUCCESS	Desired Access: G...
14:46	Explorer.EXE	8472	CreateFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Desired Access: G...
14:46	svchost.exe	2520	ReadFile	C:\Program Files\NVIDIA Corporation\...	SUCCESS	Offset: 441 344, Le...
14:46	Explorer.EXE	8472	FileSystemControl	C:\Program Files\Internet Explorer\expl...	SUCCESS	Control: FSCTL_R...
14:46	ServiceHost.exe	2476	ReadFile	C:\Program Files\McAfee\WebAdvisor\...	SUCCESS	Offset: 3 718 856, ...
14:46	aswidsagent.exe	5472	ReadFile	C:\Windows\WinSxS\FileMap\ISS_syst...	SUCCESS	Offset: 0, Length: 8...
14:46	aswidsagent.exe	5472	ReadFile	C:\Windows\WinSxS\FileMap\ISS_syst...	SUCCESS	Offset: 0, Length: 4...
14:46	Explorer.EXE	8472	CreateFileMap	C:\Program Files\Internet Explorer\expl...	FILE LOCKED WI...	SyncType: SyncTy...
14:46	Explorer.EXE	8472	QueryStandardI...	C:\Program Files\Internet Explorer\expl...	SUCCESS	AllocationSize: 819...

AutoRuns:

Megmutatja milyen programok futnak rendszerindításakor, vagy bejelentkezésakor.

Name	Description	Publisher	Image Path	Timestamp
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Fri Jan 14 10:04:57 2022
AKamai NetSession Interface			File not found: "C:\Users\User\AppData\Local\Akamai\netsession_win.e...	
com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party App...	C:\Users\User\AppData\Local\Microsoft\Teams\Update.exe	Wed Feb 9 15:43:31 2022
DAEMON Tools Lite Automount	DAEMON Tools Lite Agent	(Verified) AVB Disc Soft, SIA	C:\Program Files\DAEMON Tools Lite\DTAgent.exe	Wed Dec 23 21:27:36 2020
Discord	Update	(Verified) Discord Inc.	C:\Users\User\AppData\Local\Discord\Update.exe	Thu Dec 3 22:43:28 2020
EpicGamesLauncher	Epic Games Launcher	(Verified) Epic Games Inc.	D:\Epic Games\Epic Games Launcher\Portal\Binaries\Win64\EpicGame...	Thu Feb 17 11:27:55 2022
Skype for Desktop	Skype	(Verified) Skype Software Sarl	C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe	Fri Jan 15 21:30:30 2021
Steam	Steam	(Verified) Valve Corp.	D:\Steam\steam.exe	Sun Jan 16 18:41:26 2022
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Wed Dec 29 15:39:46 2021
AvastUI.exe	Avast AvLaunch component	(Verified) Avast Software s.r.o.	C:\Program Files\AVAST Software\Avast\AvLaunch.exe	Fri Feb 18 17:55:01 2022
Launch LCore	Logitech Gaming Framework	(Verified) Logitech Inc	C:\Program Files\Logitech Gaming Software\LCore.exe	Fri Oct 5 10:43:56 2018
RTHDVCPFL	Realtek HD Audio Manager	(Verified) Realtek Semiconductor ...	C:\Program Files\Realtek\Audio\HDA\RtkNGU64.exe	Thu Oct 23 09:35:56 2014
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	Thu Aug 22 17:37:09 2013
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Wed Oct 29 02:28:18 2014
cmd.exe				Wed Oct 29 02:28:18 2014
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Thu Feb 10 00:41:11 2022
Avast Secure Browser			File not found: "C:\Program Files (x86)\AVAST Software\Browser\Appl...	
Avast Secure Browser	Avast Browser Installer	(Verified) Avast Software s.r.o.	C:\Program Files (x86)\AVAST Software\Browser\Application\98.0.14335...	Thu Feb 24 19:55:29 2022
Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files (x86)\Google\Chrome\Application\98.0.4758.102\Insta...	Thu Feb 17 11:53:28 2022
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\83.0.478.50\Installe...	Thu Jul 9 10:48:22 2020
n/a	Microsoft .NET IE SECURITY REGISTRAT...	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Aug 17 02:06:28 2013
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				Thu Jan 13 18:17:47 2022

d)

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

```
C:\SysinternalsSuite>logonsessions -p

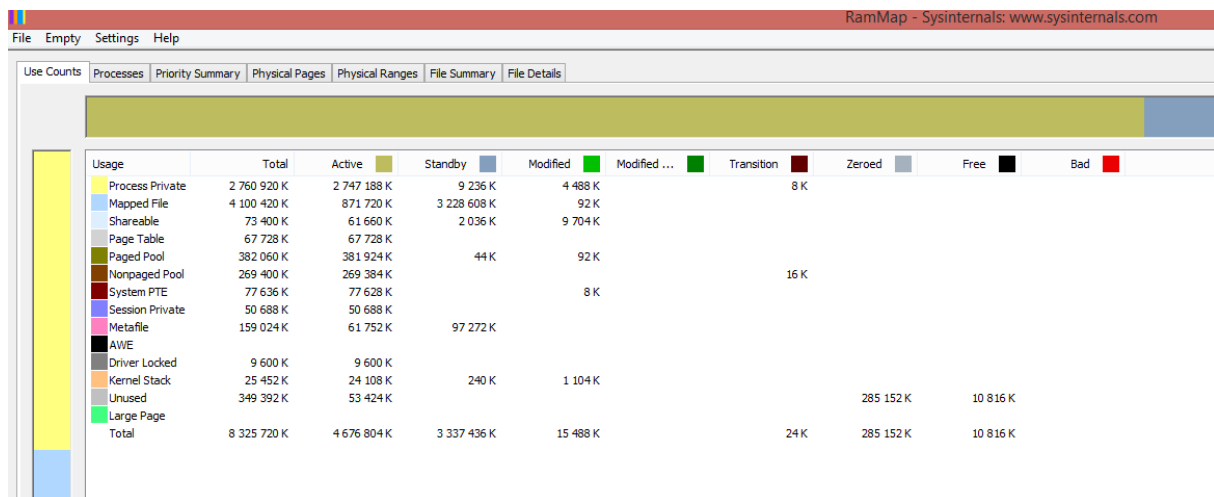
LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
User name: WORKGROUP\PC$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 2022.02.26, 10:13:11
Logon server:
DNS Domain:
UPN:
656: wininit.exe
716: lsass.exe
844: svchost.exe
1000: NVDisplay.Container.exe
856: wsc_proxy.exe
1040: svchost.exe
1132: svchost.exe
1372: AvastSvc.exe
1432: aswToolsSvc.exe
1616: spoolsv.exe
2016: armsvc.exe
1224: atkexComSvc.exe
96: aswEngSvc.exe
1748: horizon_client_service.exe
2148: svchost.exe
2200: FNPLicensingService.exe
2324: ftscamgrh.exe
2460: LogiRegistryService.exe
2476: servicehost.exe
2520: nvcontainer.exe
2848: salwriter.exe
3104: TeamViewer_Service.exe
3184: vmwsprrdpwks.exe
324: vmware-usbarbitrator64.exe
5484: AvastBrowserCrashHandler.exe
5504: AvastBrowserCrashHandler64.exe
6024: SearchIndexer.exe
5472: aswidsagent.exe
1272: Unscapp.exe
9596: DiscSoftBusServiceLite.exe
10136: BrYNSvc.exe
7744: MicrosoftEdgeUpdate.exe
12056: winlogon.exe
5248: ftnlsv.exe
8664: NVDisplay.Container.exe
10012: taskeng.exe

[1] Logon session 00000000:0000b0a5:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
```

e)

A RAMMap egy speciális fizikai memóriahasználat-elemzési segédprogram a Windows Vista és újabb verziókhoz. Különböző módokon mutatja be a használati adatokat a különböző lapjain



The screenshot shows the RAMMap application window with the 'Use Counts' tab selected. The window title is 'RamMap - Sysinternals: www.sysinternals.com'. The interface includes a menu bar (File, Empty, Settings, Help) and a tab bar (Use Counts, Processes, Priority Summary, Physical Pages, Physical Ranges, File Summary, File Details). A large horizontal bar at the top shows a memory usage distribution. Below this is a table with columns for Usage, Total, Active, Standby, Modified, Modified..., Transition, Zeroed, Free, and Bad. The table lists various memory usage categories and their corresponding values in K (Kilobytes).

Usage	Total	Active	Standby	Modified	Modified ...	Transition	Zeroed	Free	Bad
Process Private	2 760 920 K	2 747 188 K	9 236 K	4 488 K			8 K		
Mapped File	4 100 420 K	871 720 K	3 228 608 K	92 K					
Shareable	73 400 K	61 660 K	2 036 K	9 704 K					
Page Table	67 728 K	67 728 K							
Paged Pool	382 060 K	381 924 K	44 K	92 K					
Nonpaged Pool	269 400 K	269 384 K				16 K			
System PTE	77 636 K	77 628 K		8 K					
Session Private	50 688 K	50 688 K							
Metafile	159 024 K	61 752 K	97 272 K						
AWE									
Driver Locked	9 600 K	9 600 K							
Kernel Stack	25 452 K	24 108 K	240 K	1 104 K					
Unused	349 392 K	53 424 K					285 152 K	10 816 K	
Large Page									
Total	8 325 720 K	4 676 804 K	3 337 436 K	15 488 K		24 K	285 152 K	10 816 K	

3. feladat:

a) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből

File Edit View Options Profile Window Help

YEG6BLB.EXE

- KERNEL32.DLL
 - API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
 - NTDLL.DLL**
- KERNELBASE.DLL
 - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-2.DLL
 - API-MS-WIN-CORE-REGISTRY-L1-0.DLL
 - API-MS-WIN-CORE-HEAP-L1-2-0.DLL
 - API-MS-WIN-CORE-MEMORY-L1-1-2.DLL
 - API-MS-WIN-CORE-HANDLE-L1-0.DLL
 - API-MS-WIN-CORE-SYNCH-L1-2-0.DLL
 - API-MS-WIN-CORE-FILE-L1-2-1.DLL
 - API-MS-WIN-CORE-DELAYLOAD-L1-1-1.DLL
 - API-MS-WIN-CORE-IO-L1-1-1.DLL
 - API-MS-WIN-CORE-JOB-L1-1-0.DLL
 - API-MS-WIN-CORE-THREADPOOL-LEGACY-L1-1-0.DLL
 - API-MS-WIN-CORE-THREADPOOL-PRIVATE-L1-1-0.DLL
 - API-MS-WIN-CORE-LIBRARYLOADER-L1-2-0.DLL
 - API-MS-WIN-CORE-NAMEDPIPE-L1-2-0.DLL
 - API-MS-WIN-CORE-DATETIME-L1-1-1.DLL
 - API-MS-WIN-CORE-SYSINFO-L1-2-1.DLL
 - API-MS-WIN-CORE-TIMEZONE-L1-0.DLL
 - API-MS-WIN-CORE-LOCALIZATION-L1-2-1.DLL
 - API-MS-WIN-CORE-LOCALIZATION-PRIVATE-L1-1-0.DLL
 - API-MS-WIN-CORE-PROCESSENVIRONMENT-L1-2-0.DLL
 - API-MS-WIN-CORE-STRING-L1-1-0.DLL
 - API-MS-WIN-CORE-DEBUG-L1-1-1.DLL
 - API-MS-WIN-CORE-ERRORHANDLING-L1-1-1.DLL
 - API-MS-WIN-CORE-FIBERS-L1-1-1.DLL
 - API-MS-WIN-CORE-UTIL-L1-1-0.DLL
 - API-MS-WIN-CORE-PROFILE-L1-1-0.DLL
 - API-MS-WIN-CORE-SECURITY-BASE-L1-2-0.DLL
 - API-MS-WIN-CORE-COMM-L1-1-0.DLL
 - API-MS-WIN-CORE-WOW64-L1-1-0.DLL
 - API-MS-WIN-CORE-REALTIME-L1-1-0.DLL
 - API-MS-WIN-CORE-SYSTEMTOPOLOGY-L1-1-0.DLL

PI	Ordinal ^	Hint	Function	Entry Point
00000001	1 (0x0001)	N/A	N/A	Not Bound
00000019	19 (0x0013)	N/A	CsrAllocateCaptureBuffer	Not Bound
00000020	20 (0x0014)	N/A	CsrAllocateMessagePointer	Not Bound
00000025	25 (0x0019)	N/A	CsrClientCallServer	Not Bound
00000027	27 (0x001B)	N/A	CsrFreeCaptureBuffer	Not Bound
00000031	31 (0x001F)	N/A	CsrVerifyRegion	Not Bound
00000033	33 (0x0021)	N/A	DbgPrint	Not Bound
00000034	34 (0x0022)	N/A	DbgPrintEx	Not Bound
00000043	43 (0x002B)	N/A	DbgUiGetThreadDebugObject	Not Bound
00000044	44 (0x002C)	N/A	DbgUisssueRemoteBreakin	Not Bound
00000054	54 (0x0036)	N/A	EtwEventEnabled	Not Bound
00000056	56 (0x0038)	N/A	EtwEventRegister	Not Bound
00000058	58 (0x003A)	N/A	EtwEventUnregister	Not Bound
00000059	59 (0x003B)	N/A	EtwEventWrite	Not Bound
00000063	63 (0x003F)	N/A	EtwEventWriteNoRegistration	Not Bound
00000062	102 (0x0066)	N/A	LdrAddRefDll	Not Bound
00000064	104 (0x0068)	N/A	LdrDisableThreadCalloutsForDll	Not Bound
0000006A	109 (0x006D)	N/A	LdrFindResourceEx_U	Not Bound
0000006B	110 (0x006E)	N/A	LdrFindResource_U	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
00000001	1 (0x0001)	N/A	N/A	0x0000C620
00000002	2 (0x0002)	N/A	N/A	0x0000BEE0
00000003	3 (0x0003)	N/A	N/A	0x0000BF60
00000004	4 (0x0004)	N/A	N/A	0x0000BF240
00000005	5 (0x0005)	N/A	N/A	0x0000BF000
00000006	6 (0x0006)	N/A	N/A	0x000126C0
00000007	7 (0x0007)	N/A	N/A	0x0000BF300
00000008	8 (0x0008)	N/A	N/A	0x00072DC0
00000009	9 (0x0009)	661 (0x295)	RtlActivateActivationContextUnsafeFast	0x00049180
0000000A	10 (0x000A)	813 (0x32D)	RtlDeactivateActivationContextUnsafeFast	0x00049210
0000000B	11 (0x000B)	1063 (0x427)	RtlInterlockedPushListSList	0x0002A890
0000000C	12 (0x000C)	1355 (0x54B)	RtlUlongByteSwap	0x0002A930
0000000D	13 (0x000D)	1356 (0x54C)	RtlUlonglongByteSwap	0x0002A940
0000000E	14 (0x000E)	1396 (0x574)	RtlUshortByteSwap	0x0002A920
0000000F	15 (0x000F)	89 (0x0059)	ExInterlockedPopEntrySListEnd	0x0002A844
00000010	16 (0x0010)	90 (0x005A)	ExInterlockedPopEntrySListFault	0x0002A84C
00000011	17 (0x0011)	91 (0x005B)	ExInterlockedPopEntrySListResume	0x00008370
00000012	18 (0x0012)	0 (0x0001)	A_SHAFinal	0x00008370
00000013	19 (0x0013)	1 (0x0001)	A_SHAFinal	0x00008350