

Operációs rendszerek BSC

1. Gyak.

2022.03.12

Készítette:

Salamon István BSC

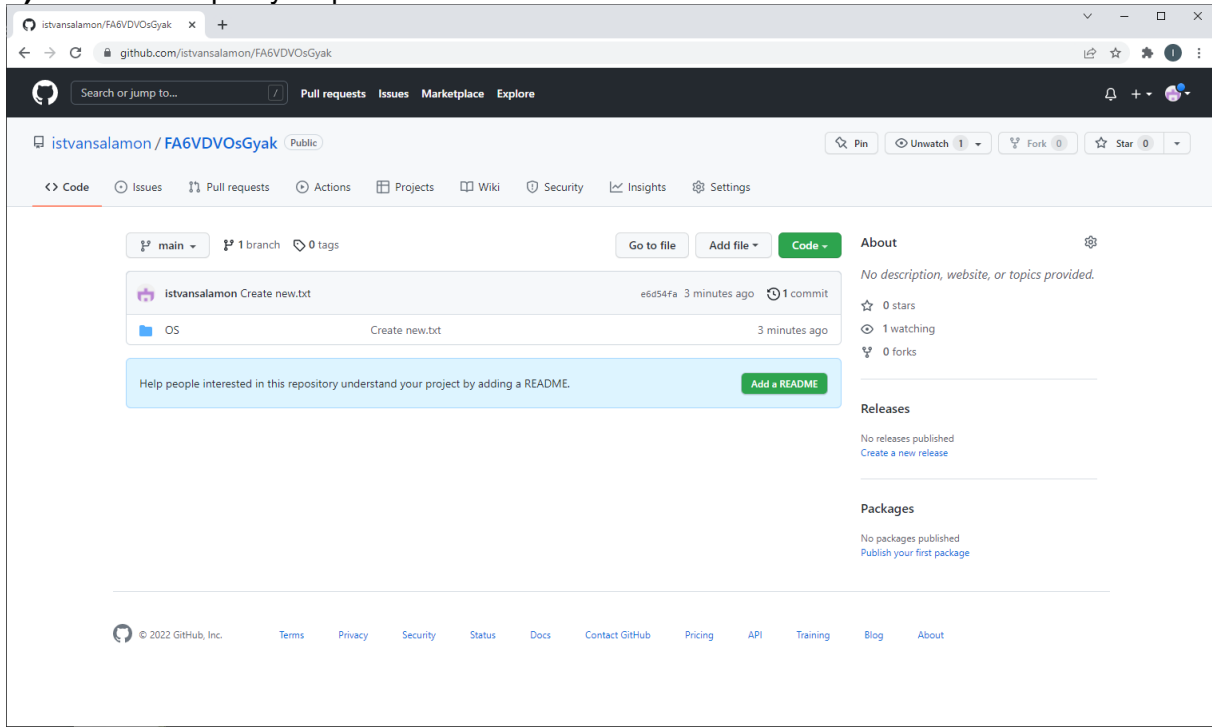
Mérnökinformatikus szak

FA6VDV

Miskolc, 2022

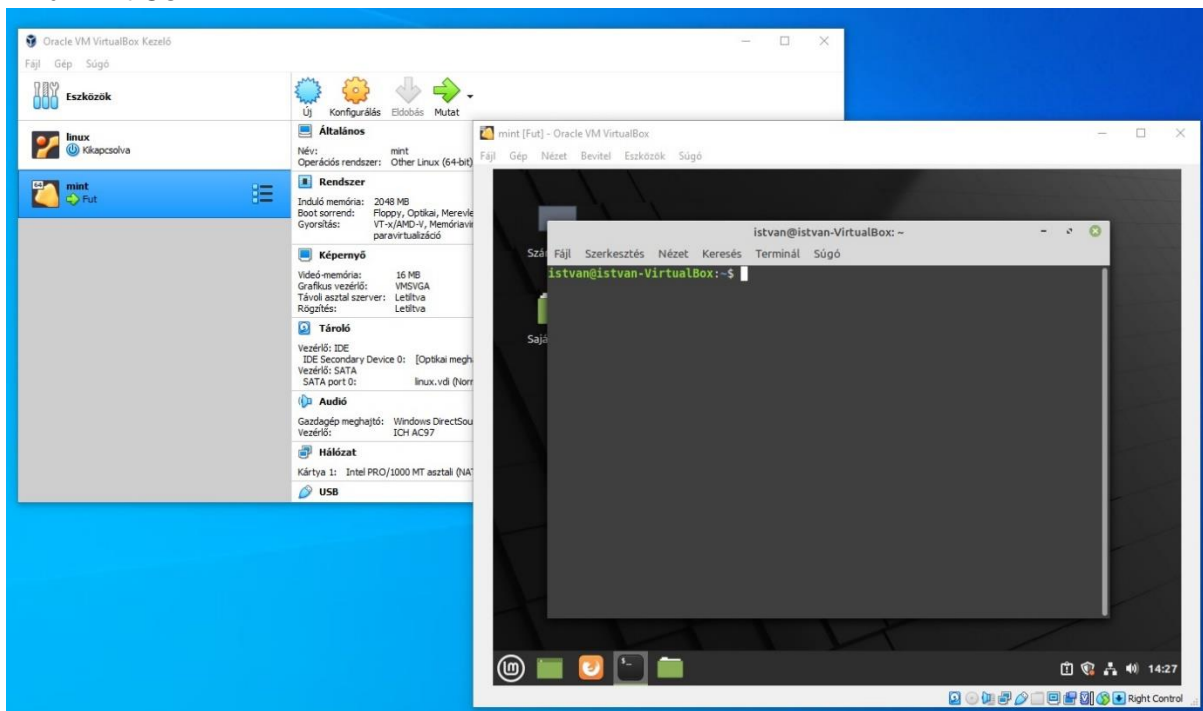
1. **Feladat:** GitHub fiók, repository létrehozása.
2. **Feladat:** Laborhasználati szabályzat elolvasása
3. **Feladat:** Linux disztribúció virtuális gép létrehozása VirtualBoxszal
4. **Feladat:**

a) Készítsen képernyőképet a GitHub fiókról:



<https://github.com/istvansalamon/FA6VDVOsGyak/>

b) Készítsen képernyőképet belépés után a konzolos felületről a VirtualBoxra telepített LinuxMint Os – lehet más disztribúció is.

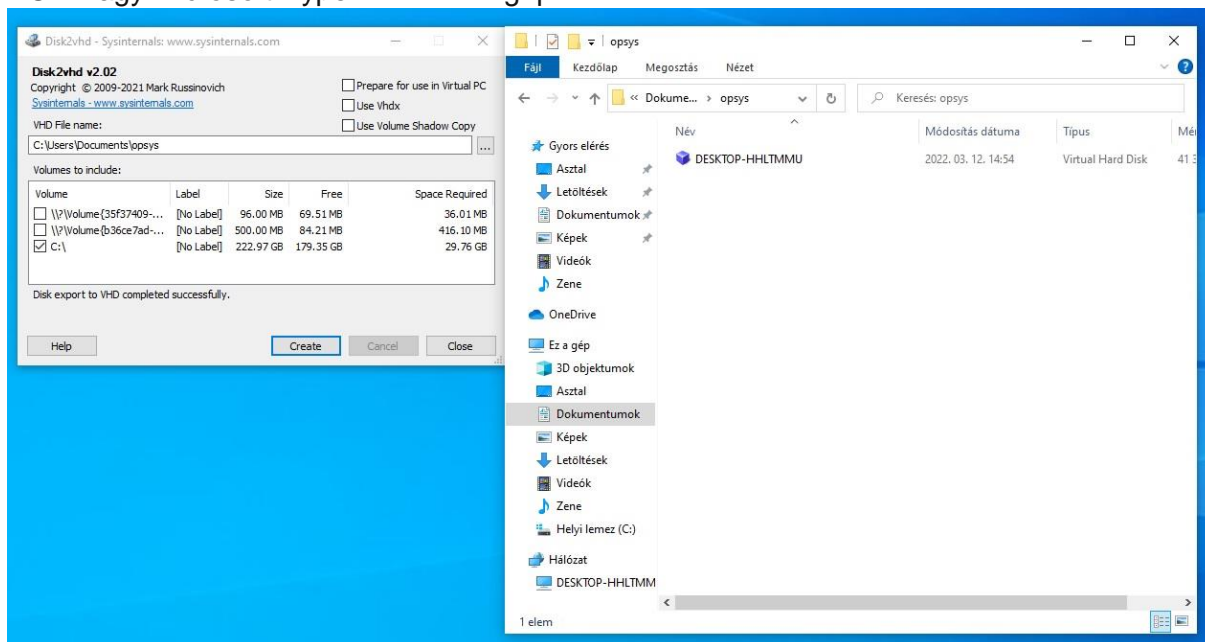


5. feladat

Töltse le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít. A felsorolt eszközök közül minden eszköz esetén töltse le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét - majd mentse el a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).

a) File and Disk Utilities (Disk2vhd)

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

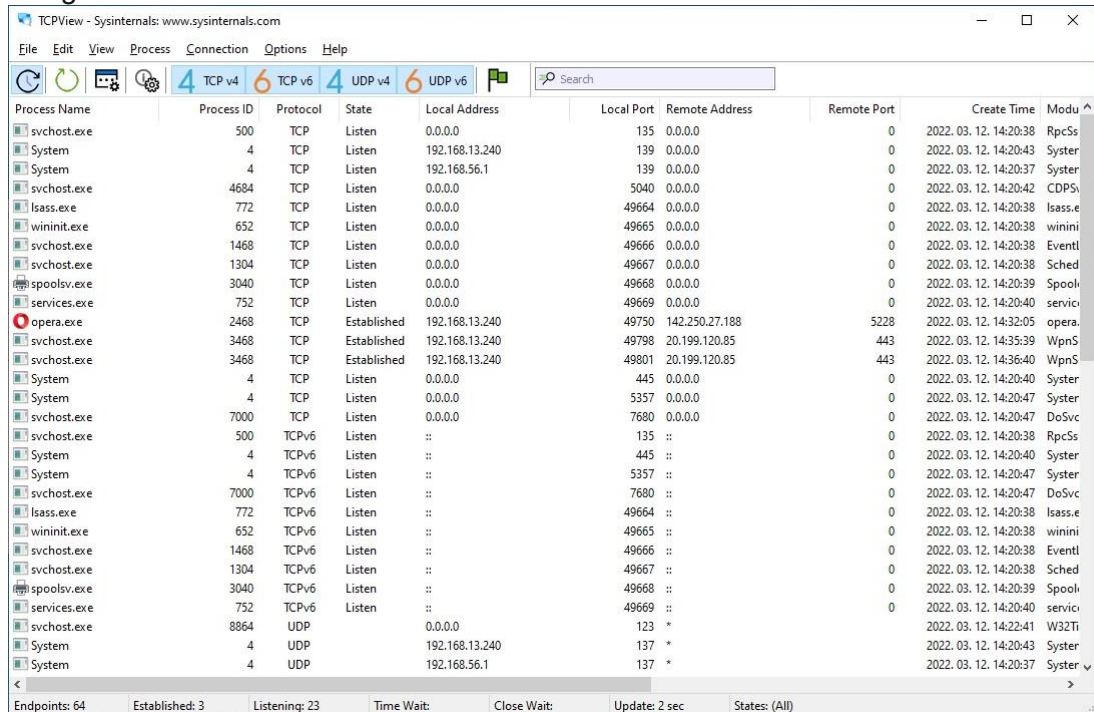


b) Networking Utilities (TCPView)

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

használatát:

A TCPView indítani fogja az összes aktív TCP- és UDP-végpont felsorolását, és feloldja az összes IP-címet a tartománynév-verziójukra. Eszköztárgomb vagy menüelem használatával válthat a feloldott nevek megjelenítésére. A TCPView megjeleníti az egyes végpontok tulajdonában következő folyamat nevét, beleértve a szolgáltatás nevét is



The screenshot shows the TCPView application window with the following data:

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Modu
svchost.exe	500	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.03.12.14:20:38	RpcSs
System	4	TCP	Listen	192.168.13.240	139	0.0.0.0	0	2022.03.12.14:20:43	Syster
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.03.12.14:20:37	Syster
svchost.exe	4684	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.03.12.14:20:42	CDPS
lsass.exe	772	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.03.12.14:20:38	lsass.e
wininit.exe	652	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.03.12.14:20:38	winini
svchost.exe	1468	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.03.12.14:20:38	Eventl
svchost.exe	1304	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022.03.12.14:20:38	Sched
spoolsv.exe	3040	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2022.03.12.14:20:39	Spool
services.exe	752	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	2022.03.12.14:20:40	servic
opera.exe	2468	TCP	Established	192.168.13.240	49750	142.250.27.188	5228	2022.03.12.14:32:05	opera.
svchost.exe	3468	TCP	Established	192.168.13.240	49798	20.199.120.85	443	2022.03.12.14:35:39	WpnS
svchost.exe	3468	TCP	Established	192.168.13.240	49801	20.199.120.85	443	2022.03.12.14:36:40	WpnS
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	2022.03.12.14:20:40	Syster
System	4	TCP	Listen	0.0.0.0	5357	0.0.0.0	0	2022.03.12.14:20:47	Syster
svchost.exe	7000	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	2022.03.12.14:20:47	DoSvc
svchost.exe	500	TCPv6	Listen	::	135	::	0	2022.03.12.14:20:38	RpcSs
System	4	TCPv6	Listen	::	445	::	0	2022.03.12.14:20:40	Syster
System	4	TCPv6	Listen	::	5357	::	0	2022.03.12.14:20:47	Syster
svchost.exe	7000	TCPv6	Listen	::	7680	::	0	2022.03.12.14:20:47	DoSvc
lsass.exe	772	TCPv6	Listen	::	49664	::	0	2022.03.12.14:20:38	lsass.e
wininit.exe	652	TCPv6	Listen	::	49665	::	0	2022.03.12.14:20:38	winini
svchost.exe	1468	TCPv6	Listen	::	49666	::	0	2022.03.12.14:20:38	Eventl
svchost.exe	1304	TCPv6	Listen	::	49667	::	0	2022.03.12.14:20:38	Sched
spoolsv.exe	3040	TCPv6	Listen	::	49668	::	0	2022.03.12.14:20:39	Spool
services.exe	752	TCPv6	Listen	::	49669	::	0	2022.03.12.14:20:40	servic
svchost.exe	8864	UDP		0.0.0.0	123	*		2022.03.12.14:22:41	W32Ti
System	4	UDP		192.168.13.240	137	*		2022.03.12.14:20:43	Syster
System	4	UDP		192.168.56.1	137	*		2022.03.12.14:20:37	Syster

Summary: Endpoints: 64, Established: 3, Listening: 23, Time Wait: , Close Wait: , Update: 2 sec, States: (All)

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

Process Explorer

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

A *Process Explorer* egy hatékony keresési képességgel is rendelkezik, amely gyorsan megmutatja, hogy mely folyamatokhoz vannak megnyitva adott leírók vagy betöltött CL-ek.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-HHLTMMU\fa]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		7 740 K	20 988 K	108		
System Idle Process	96.64	60 K	8 K	0		
System	< 0.01	200 K	620 K	4		
Interrupts	0.38	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 072 K	396 K	420		
Memory Compression		268 K	28 856 K	2428		
csrss.exe		1 676 K	1 892 K	524		
wininit.exe		1 356 K	912 K	652		
services.exe		5 024 K	6 204 K	752		
svchost.exe		9 908 K	17 792 K	976	Windows-szolgáltatások gaz...	Microsoft Corporation
Start Menu Experience...		32 376 K	43 316 K	5872		
RuntimeBroker.exe		5 732 K	16 340 K	6080	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	110 428 K	104 164 K	5216	Search application	Microsoft Corporation
RuntimeBroker.exe		14 620 K	16 844 K	5396	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2 988 K	3 712 K	8020	Runtime Broker	Microsoft Corporation
VBoxSVC.exe	< 0.01	6 496 K	8 592 K	8436	VirtualBox Interface	Oracle Corporation
VirtualBox VM.exe		1 924 K	1 252 K	9168	VirtualBox Virtual Machine	Oracle Corporation
VirtualBox VM.exe		1 972 K	888 K	9192	VirtualBox Virtual Machine	Oracle Corporation
VirtualBox V...	0.38	105 528 K	87 600 K	9200	VirtualBox Virtual Machine	Oracle Corporation
TextInputHost.exe		15 752 K	14 876 K	3672		Microsoft Corporation
dllhost.exe		3 728 K	3 352 K	4444	COM Surrogate	Microsoft Corporation
UserOOBEBroker.exe		1 912 K	4 368 K	7728	User OOBEBroker	Microsoft Corporation
ShellExperienceHost...	Susp...	25 320 K	16 796 K	2268	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		1 872 K	1 788 K	3200	Runtime Broker	Microsoft Corporation
Microsoft.Photos.exe	Susp...	55 832 K	5 248 K	4256		
RuntimeBroker.exe		9 576 K	14 108 K	5656	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	34 056 K	20 468 K	4172		Microsoft Corporation
RuntimeBroker.exe		2 000 K	5 240 K	1764	Runtime Broker	Microsoft Corporation
WmiPrvSE.exe		2 684 K	9 348 K	8756		

CPU Usage: 2.63% Commit Charge: 45.48% Processes: 149 Physical Usage: 45.07%

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 kipurító szűrést, átfogó eseménytulajdonságokat, például munkamenet-azonosítókat és felhasználóneveket, megbízható folyamatinformációkat, teljes szálkészleteket az egyes műveletek integrált szimbólumtámogatásával, a fájlba történő egyidejű naplózást.

Process Monitor - Sysinternals: www.sysinternals.com

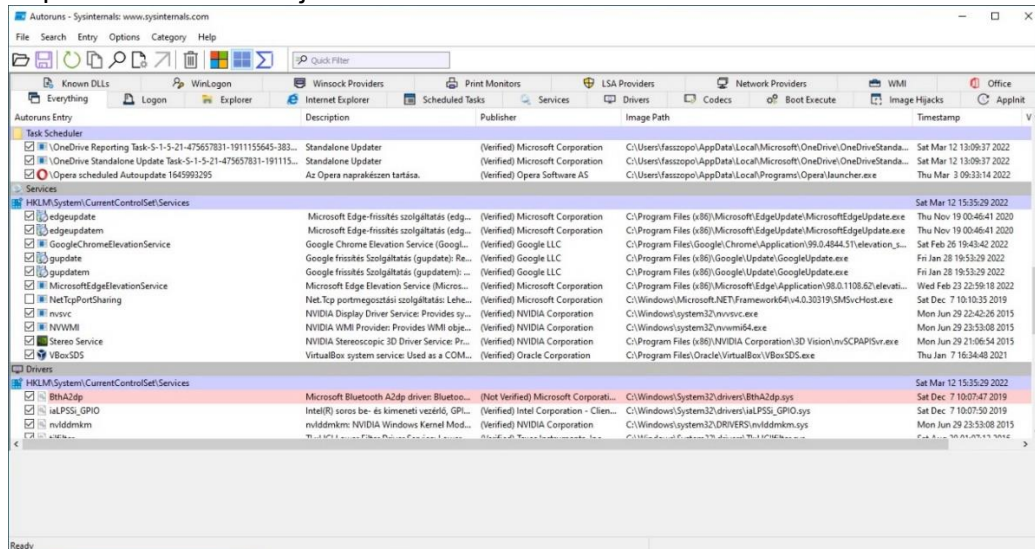
File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
15:35...	svchost.exe	2816	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690 688, Le...
15:35...	svchost.exe	2816	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 678 400, Le...
15:35...	svchost.exe	2816	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 635 904, Le...
15:35...	lsass.exe	772	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 2 530 816, ...
15:35...	svchost.exe	2816	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 627 712, Le...
15:35...	lsass.exe	772	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 607 168, ...
15:35...	svchost.exe	2816	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
15:35...	lsass.exe	772	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 590 784, ...
15:35...	svchost.exe	2816	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 611 328, Le...
15:35...	lsass.exe	772	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 505 280, ...
15:35...	Explorer.EXE	5056	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query Name
15:35...	Explorer.EXE	5056	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query HandleTag...
15:35...	lsass.exe	772	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 578 496, ...
15:35...	Explorer.EXE	5056	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query HandleTag...
15:35...	Explorer.EXE	5056	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
15:35...	Explorer.EXE	5056	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
15:35...	lsass.exe	772	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 488 896, ...
15:35...	Explorer.EXE	5056	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query Name
15:35...	lsass.exe	772	QueryNameInfo	C:\Users\Yassozo\Downloads\Synter...	SUCCESS	Name: \Users\Yass...
15:35...	lsass.exe	772	QueryNameInfo	C:\Users\Yassozo\Downloads\Synter...	SUCCESS	Name: \Users\Yass...
15:35...	svchost.exe	2816	QueryStandard...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3 1...
15:35...	svchost.exe	2816	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 590 784, ...
15:35...	Explorer.EXE	5056	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query HandleTag...
15:35...	Explorer.EXE	5056	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
15:35...	Explorer.EXE	5056	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
15:35...	ctfmon.exe	4512	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offset: 4 031 488, ...
15:35...	svchost.exe	2816	UnloadFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123 368, Le...
15:35...	Explorer.EXE	5056	CreateFile	C:\Users\Yassozo\Downloads\Synter...	SUCCESS	Desired Access: R...
15:35...	ctfmon.exe	4512	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offset: 4 019 200, ...
15:35...	Explorer.EXE	5056	QueryBasicInfo	C:\Users\Yassozo\Downloads\Synter...	SUCCESS	CreationTime: 202...
15:35...	Explorer.EXE	5056	CreateFile	C:\Users\Yassozo\Downloads\Synter...	SUCCESS	Offset: 4 088 832, ...
15:35...	ctfmon.exe	4512	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	AllocationSize: 262...
15:35...	Explorer.EXE	5056	QueryStandard...	C:\Users\Yassozo\AppData\Local\Loc...	SUCCESS	Offset: 899 584, Le...
15:35...	ctfmon.exe	4512	ReadFile	C:\Windows\System32\TextInputFrame...	SUCCESS	Offset: 3 022 336, ...
15:35...	Explorer.EXE	5056	CreateFile	C:\Users\Yassozo\Downloads\Synter...	SUCCESS	Desired Access: R...
15:35...	Explorer.EXE	5056	QueryBasicInfo	C:\Users\Yassozo\Downloads\Synter...	SUCCESS	CreationTime: 202...
15:35...	Explorer.EXE	5056	CreateFile	C:\Users\Yassozo\Downloads\Synter...	SUCCESS	Offset: 4 088 832, ...
15:35...	ctfmon.exe	4512	RegQueryValue	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query HandleTag...
15:35...	ctfmon.exe	4512	RegOpenKey	HKCU\Software\Microsoft\Windows\A...	SUCCESS	Desired Access: R...
15:35...	ctfmon.exe	4512	RegQueryValue	HKCU\Software\Microsoft\Windows\A...	SUCCESS	Query HandleTag...

Showing 33 718 of 277 638 events (19%) Backed by virtual memory

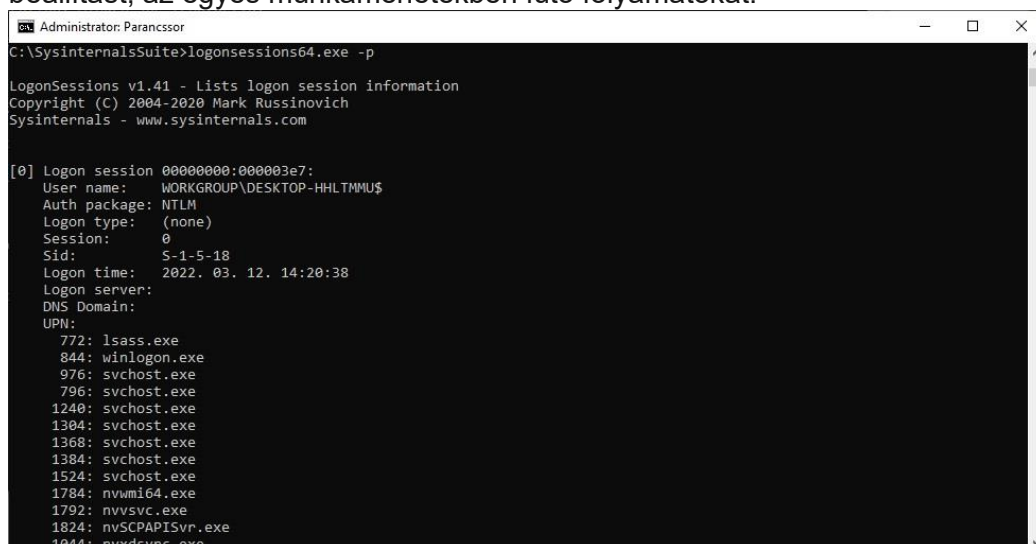
Autoruns

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 Explorert és a médialejátszókat.



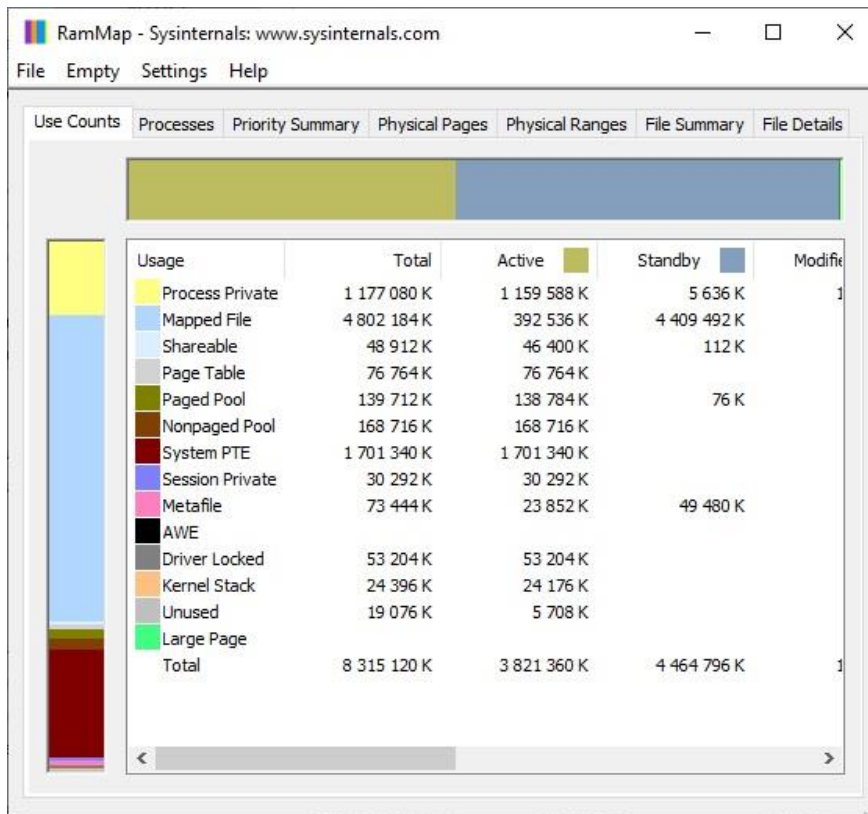
d) Security Utilities (LogonSession)

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



e) Information Utilities (RAMMap)

RaMMap: A RAMMap egy speciális fizikai memóriahasználat-elemzési segédprogram. Megmutatja, hogy a Windows hogyan rendel fizikai memóriát és mennyi fájladat van gyorsítótárazva a RAM-ban, vagy mennyi memóriát használ a kernel és az eszközillesztők.



Feladat

A) Készítse el a következő feladatokat!

1. Hozza létre a következő jegyzék szerkezetet, majd listázza ki

```
istvan@istvan-VirtualBox:~/Dokumentumok$ tree
```

```

├── fa6vdv
│   ├── bush
│   │   ├── banan
│   │   ├── barack
│   │   └── mogyoro
│   ├── land
│   │   ├── kokusz
│   │   └── szeder
│   └── tree
│       └── korte

```

```
10 directories, 0 files
```

```
istvan@istvan-VirtualBox:~/Dokumentumok$
```

2. Készítsen másolatot:
 - a neptunkod/ land/szeder katalógusról a neptunkod/tree katalógusba

```

istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ cp -R land/szeder tree/
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ tree
.
├── bush
│   ├── banan
│   ├── barack
│   └── mogyoro
├── land
│   ├── kokusz
│   └── szeder
└── tree
    ├── korte
    └── szeder

10 directories, 0 files
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$

```

- a neptunkod /bush/banan katalógusról a neptunkod /tree katalógusba

```

istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ cp -R bush/banan tree/
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ tree
.
├── bush
│   ├── banan
│   ├── barack
│   └── mogyoro
├── land
│   ├── kokusz
│   └── szeder
└── tree
    ├── banan
    ├── korte
    └── szeder

11 directories, 0 files
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$

```

3. Végezze el a következő áthelyezéseket:

- a neptunkod / bush /barack katalógust helyezze át a neptunkod /tree katalógusba

```

istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ mv bush/barack/ tree/
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ tree
.
├── bush
│   ├── banan
│   └── mogyoro
├── land
│   ├── kokusz
│   └── szeder
└── tree
    ├── banan
    ├── barack
    ├── korte
    └── szeder

11 directories, 0 files
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$

```


- a neptunkod /land /kokusz katalógust helyezze át a neptunkod/tree katalógusba

```
11 directories, 0 files
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ mv land/kokusz/ tree/
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ tree
.
├── bush
│   ├── banan
│   └── mogyoro
├── land
│   └── szeder
└── tree
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder

11 directories, 0 files
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$
```

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

```
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ rm -rf land/
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ tree
.
├── bush
│   ├── banan
│   └── mogyoro
└── tree
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder

9 directories, 0 files
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$
```

- neptunkod/bush/banan/ description
- neptunkod/tree/listing

5. A description szöveges állományba írjon 3 sort a málnáról. A listing szöveges állományba soroljon fel külön sorba 5 olyan gyümölcsöt, amelyek tree teremnek

```
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/bush$ cd banan
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/bush/banan$ nano description.txt
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/bush/banan$ cat description.txt
A málna a Dunántúl egyes részein elterjedt népies nevén a 'Boldogasszony
csipkéje'.
és a himpér a német Himbeere szó alapján.
Magyarországon őshonos, föld alatti tarackokat hajtó, kb. 2 m magasfélcserje.
Májustól augusztusig virágzik.

istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/tree$ nano listing.txt
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/tree$ cat listing.txt
alma
barack
kokusz
korte
szilva
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/tree$
```

6. Listázza a neptunkod katalógus tartalmát úgy, hogy megjelenjen az alkatalógusok tartalma is. Ezután listázza az aktuális (munka)katalógus nevét.

```
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$ tree -f
.
├── ./bush
│   ├── ./bush/banan
│   │   └── ./bush/banan/description.txt
│   └── ./bush/mogyoro
└── ./tree
    ├── ./tree/banan
    ├── ./tree/barack
    ├── ./tree/kokusz
    ├── ./tree/korte
    ├── ./tree/listing.txt
    └── ./tree/szeder

9 directories, 2 files
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv$
```

7. . Térjen vissza a saját home katalógusába és keresse meg az összes olyan file-t, amelyek nevének második betűje e.

```
istvan@istvan-VirtualBox:~$ ls -R | grep "^e"
Leletések
Zenék
description.txt
istvan@istvan-VirtualBox:~$
```

8. Tegye mindenki számára olvashatóvá a listing file-t.

```
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/tree$ ls -l listing.txt
-rw-rw-r-- 1 istvan istvan 32 márc 12 16:21 listing.txt
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/tree$ chmod a+rx listing.txt
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/tree$ ls -l listing.txt
-rwxrwxrwx 1 istvan istvan 32 márc 12 16:21 listing.txt
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/tree$
```

9. .Listázza ki, hogy mennyi helyet foglal a merevlemezén a neptunkód katalógus az alkatalógusaival együtt. Az alkatalógusok méretei ne jelenjenek meg.

```
istvan@istvan-VirtualBox:~$ du -csbh Dokumentumok/fa6vdv
41K    Dokumentumok/fa6vdv
41K    total
istvan@istvan-VirtualBox:~$
```

10. . Listázza ABC-szerint rendezve a listing file tartalmát.

```
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/tree$ sort listing.txt
alma
barack
kokusz
korte
szilva
```

11. Számolja meg a description file-ban szereplő szavakat.

```
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/bush/banan$ wc -lwm description.txt
5 33 236 description.txt
istvan@istvan-VirtualBox:~/Dokumentumok/fa6vdv/bush/ba
```