

Operációs rendszerek BSc

2. Gyak.

2022. 02. 15.

Készítette:

Szendrei GáborBsc

Programtervező informatikus

V9ZK10

Miskolc, 2022

1. feladat

a) Hozza létre a következő mappa szerkezetet!

```
Administrator: Command Prompt
E:\legyetem\Oprendszer>cd V92K18
E:\legyetem\Oprendszer\V92K18>mkdir bokor
E:\legyetem\Oprendszer\V92K18>mkdir fa
E:\legyetem\Oprendszer\V92K18>mkdir land
E:\legyetem\Oprendszer\V92K18>cd bokor
E:\legyetem\Oprendszer\V92K18\bokor>mkdir banan
E:\legyetem\Oprendszer\V92K18\bokor>mkdir megjoro
E:\legyetem\Oprendszer\V92K18\bokor>mkdir barack
E:\legyetem\Oprendszer\V92K18\bokor>cd..
E:\legyetem\Oprendszer\V92K18>cd fa
E:\legyetem\Oprendszer\V92K18\fa>mkdir korte
E:\legyetem\Oprendszer\V92K18\fa>mkdir..
E:\legyetem\Oprendszer\V92K18>cd land
E:\legyetem\Oprendszer\V92K18\land>mkdir szeder
E:\legyetem\Oprendszer\V92K18\land>mkdir kokusz
E:\legyetem\Oprendszer\V92K18\land>cd..
E:\legyetem\Oprendszer\V92K18>tree
Folder PATH listing
Volume serial number is 7EC9-6498
F:.
|-- bokor
|   |-- banan
|   |-- barack
|   |-- megjoro
|   -- fa
|       |-- korte
|       -- land
|           |-- kokusz
|           -- szeder
--..
E:\legyetem\Oprendszer\V92K18>
```

b) Készítsen másolatot:

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

```
Administrator: Command Prompt
E:\legyetem\Oprendszer\V92K18>xcopy land fa /E /T
E:\legyetem\Oprendszer\V92K18>tree
Folder PATH listing
Volume serial number is 7EC9-6498
F:.
|-- bokor
|   |-- banan
|   |-- barack
|   |-- megjoro
|   -- fa
|       |-- korte
|       -- land
|           |-- kokusz
|           -- szeder
--..
E:\legyetem\Oprendszer\V92K18>
```

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

```
Select Administrator Command Prompt
E:\legyetem\oprendszer\V9ZK10>copy bokor fa /t /y
E:\legyetem\oprendszer\V9ZK10>tree
Folder PATH listing
Volume serial number is 7EC9-E498
D:\
├── bokor
│   ├── banan
│   ├── barack
│   └── meggy
├── fa
│   ├── banan
│   ├── korte
│   ├── szeder
│   └── land
├── kokusz
└── szeder
E:\legyetem\oprendszer\V9ZK10>
```

c) Végezze el a következő áthelyezéseket:

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

```
Administrator Command Prompt
E:\legyetem\oprendszer\V9ZK10>move bokor\barack fa
1 dir(s) moved.
E:\legyetem\oprendszer\V9ZK10>tree
Folder PATH listing
Volume serial number is 7EC9-E498
D:\
├── bokor
│   ├── banan
│   └── meggy
├── fa
│   ├── banan
│   ├── barack
│   ├── korte
│   ├── szeder
│   └── land
├── kokusz
└── szeder
E:\legyetem\oprendszer\V9ZK10>
```

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

```
Administrator: Command Prompt
E:\legyetem\Oprendszer\V92K18>move land\kokusz fa
1 dir(s) moved.

E:\legyetem\Oprendszer\V92K18>tree
Folder PATH listing
Volume serial number is 7EC9-E498
E:.
|-- bokor
|   |-- banan
|   |-- megynono
|   |-- fa
|       |-- banan
|       |-- barack
|       |-- kokusz
|       |-- korte
|       |-- szeder
|-- land
|   |-- szeder

```

d) Törölje a neptunkod/land katalógust a teljes tartalmával.

Hozza létre a következő szöveges állományokat:

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

```
Administrator: Command Prompt
E:\legyetem\Oprendszer\V92K18>rmdir /s land
land, Are you sure (Y/N)? y

E:\legyetem\Oprendszer\V92K18>tree
Folder PATH listing
Volume serial number is 7EC9-E498
E:.
|-- bokor
|   |-- banan
|   |-- megynono
|   |-- fa
|       |-- banan
|       |-- barack
|       |-- kokusz
|       |-- korte
|       |-- szeder

```

```
E:\legyetem\Oprendszer\V92K18>cd bokor\banan
E:\legyetem\Oprendszer\V92K18\bokor\banan>copy nul > leiras.txt
E:\legyetem\Oprendszer\V92K18\bokor\banan>cd..
E:\legyetem\Oprendszer\V92K18\bokor>cd..
E:\legyetem\Oprendszer\V92K18>cd fa
E:\legyetem\Oprendszer\V92K18\fa>copy nul > felsorolas.txt
E:\legyetem\Oprendszer\V92K18\fa>
```

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

A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

```
Administrator: Command Prompt
E:\legyetem\Oprendszer\V92K10\bokor\banan>copy con leiras.txt
Serge
Overwrite leiras.txt? (Yes/No/All): y
Dzsi
Kajszl
1 file(s) copied.
E:\legyetem\Oprendszer\V92K10\bokor\banan>cd..
E:\legyetem\Oprendszer\V92K10\bokor>cd..
E:\legyetem\Oprendszer\V92K10>cd fa
E:\legyetem\Oprendszer\V92K10\fa>copy con felsorolas.txt
Mate
Roll
Kristof
Viktor
Metyl
1 file(s) copied.
E:\legyetem\Oprendszer\V92K10\fa>
```

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

```
Administrator: Command Prompt
E:\legyetem\Oprendszer>tree /F
Folder PATH listing
Volume serial number is 7C93-6498
E:.
jegyzokonyv minta.docx
V92K10_0211.pdf
V92K10
├── bokor
│   ├── banan
│   └── leiras.txt
├── egyyoro
├── fa
│   └── felsorolas.txt
├── banan
├── barack
├── bokor
├── korte
└── szeder
E:\legyetem\Oprendszer>
```

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

```
Administrator Command Prompt
E:\legyetem\Oprendszer\V92K10>dir /S /e*
Volume in drive E has no label.
Volume Serial Number is 7E5B-E498

Directory of E:\legyetem\Oprendszer\V92K10\borok\banan

17/02/2022  08:12                21 leiras.txt
               1 File(s)                21 bytes

Directory of E:\legyetem\Oprendszer\V92K10\fa

17/02/2022  08:12                36 felsorolas.txt
               1 File(s)                36 bytes

Total Files Listed:
                2 File(s)                57 bytes
                0 Dir(s) 35,317,878 bytes free

E:\legyetem\Oprendszer\V92K10>
```

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

```
Administrator Command Prompt
E:\legyetem\Oprendszer\V92K10>cd fa
E:\legyetem\Oprendszer\V92K10\fa>attrib +r felsorolas.txt
E:\legyetem\Oprendszer\V92K10\fa>
```

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

```
Administrator Command Prompt

Directory of E:\vegyes\Oprendszer\V92K10\bokor\banan
17/02/2022 08:11 <DIR> .
17/02/2022 08:03 <DIR> ..
17/02/2022 08:12 21 feliras.txt 21 bytes
1 File(s)
0 File(s) 0 bytes

Directory of E:\vegyes\Oprendszer\V92K10\bokor\magyofo
17/02/2022 07:48 <DIR> .
17/02/2022 08:03 <DIR> ..
0 File(s) 0 bytes

Directory of E:\vegyes\Oprendszer\V92K10\fa
17/02/2022 08:13 <DIR> .
17/02/2022 08:08 <DIR> ..
17/02/2022 07:48 <DIR> banan
17/02/2022 07:48 <DIR> barack
17/02/2022 08:12 36 felsorolas.txt
17/02/2022 07:48 <DIR> kokusz
17/02/2022 07:48 <DIR> korte
17/02/2022 07:48 <DIR> szeder
1 File(s) 36 bytes

Directory of E:\vegyes\Oprendszer\V92K10\fa\banan
17/02/2022 07:48 <DIR> .
17/02/2022 08:13 <DIR> ..
0 File(s) 0 bytes

Directory of E:\vegyes\Oprendszer\V92K10\fa\barack
17/02/2022 07:48 <DIR> .
17/02/2022 08:13 <DIR> ..
0 File(s) 0 bytes

Directory of E:\vegyes\Oprendszer\V92K10\fa\kokusz
17/02/2022 07:48 <DIR> .
17/02/2022 08:13 <DIR> ..
0 File(s) 0 bytes

Directory of E:\vegyes\Oprendszer\V92K10\fa\korte
17/02/2022 07:48 <DIR> .
17/02/2022 08:13 <DIR> ..
0 File(s) 0 bytes

Directory of E:\vegyes\Oprendszer\V92K10\fa\szeder
17/02/2022 07:48 <DIR> .
17/02/2022 08:13 <DIR> ..
0 File(s) 0 bytes

Total Files Listed:
5 File(s) 387,618 bytes
32 Dir(s) 35,317,878,784 bytes free

E:\vegyes\Oprendszer>
```

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

```
Administrator Command Prompt

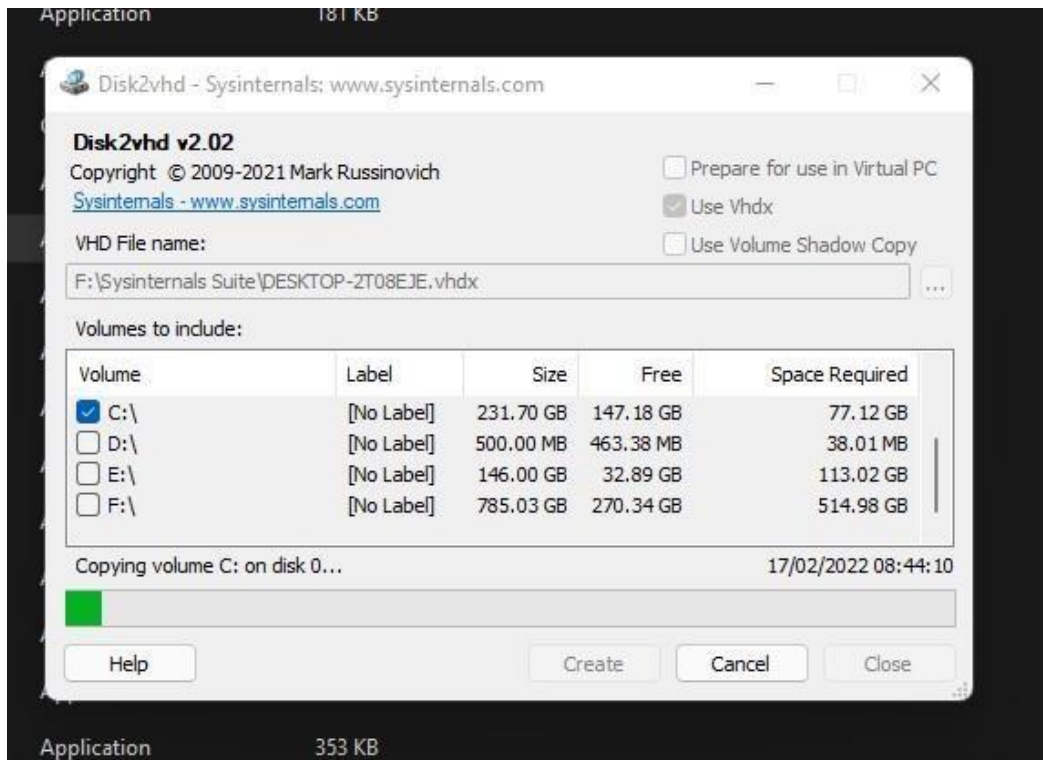
E:\vegyes\Oprendszer\V92K10\fa>sort felsorolas.txt
Viktor
Mata
Matyi
Roli
Viktor

E:\vegyes\Oprendszer\V92K10\fa>
```

2. Tölts le a Sysinternals Suite csomagot, majd csomagolja ki.

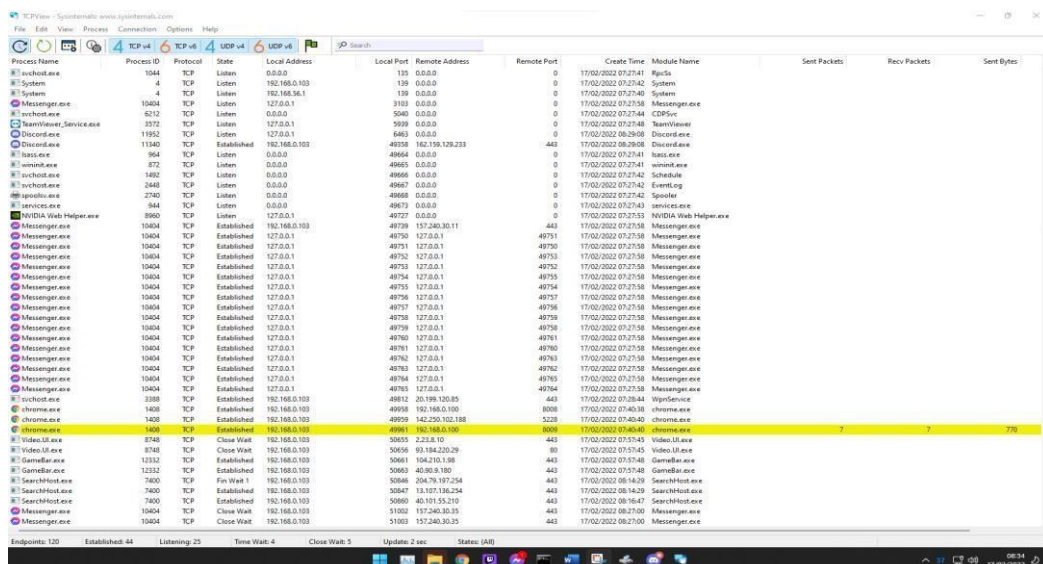
a) File and Disk Utilities (Disk2vhd)

Egy fájlba Lementi a teljes meghajtó tartalmát. Biztonsági mentést készít róla



b) Networking Utilities (TCPView)

A futó alkalmazásoknak listázza a TCP és UDP csatlakozás végpontjait a lokális és távoli címeiket és a tcp csatlakozás állapotát



File Options View Process Find Users Help

CPU: 1.39% Private Bytes: 45,648 K Working Set: 200 PID: Description Company Name

-Filter by name

	CPU	Private Bytes	Working Set	PID	Description	Company Name
[+] System Idle Process	97.63	60 K	8 K	0		
[+] System	<0.01	56 K	1,112 K	4		
[+] smss.exe	<0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
[+] csrss.exe	1,080 K	1,140 K	608			
[+] Memory Compression	636 K	184,572 K	2616			
[+] csrss.exe	2,160 K	5,728 K	788			
[+] wscntest.exe	1,342 K	6,604 K	872			
[+] services.exe	6,148 K	14,632 K	944			
[+] smss.exe	<0.01	12,420 K	32,012 K	764	Host Process for Windows S... Microsoft Corporation	
[+] csrss.exe	<0.01	84,416 K	85,212 K	780		
[+] SearchIndexer.exe	Susp.	313,776 K	343,260 K	760		Microsoft Corporation
[+] RuntimeBroker.exe		6,684 K	27,460 K	762	Runtime Broker	Microsoft Corporation
[+] RuntimeBroker.exe		17,036 K	58,564 K	778	Runtime Broker	Microsoft Corporation
[+] shost.exe		9,592 K	18,000 K	814	COM Surrogate	Microsoft Corporation
[+] csrss.exe	Susp.	84,208 K	85,212 K	780		Microsoft Corporation
[+] RuntimeBroker.exe		2,820 K	18,660 K	548	Runtime Broker	Microsoft Corporation
[+] shost.exe		3,584 K	11,240 K	574		
[+] RuntimeBroker.exe	<0.01	19,540 K	38,560 K	1188	Application Frame Host	Microsoft Corporation
[+] shost.exe		2,408 K	13,960 K	1190	COM Surrogate	Microsoft Corporation
[+] RuntimeBroker.exe		6,544 K	26,244 K	1204	Runtime Broker	Microsoft Corporation
[+] shost.exe		1,980 K	13,172 K	4392	COM Surrogate	Microsoft Corporation
[+] Battle.net.exe	Susp.	72,060 K	130,64 K	1223	Battle Game Bar	Microsoft Corporation
[+] ksmcui.dll	Susp.	73,364 K	13,024 K	636		
[+] CamStudio Server.exe		2,584 K	13,664 K	9143	Xbox Game Bar Full Trust C...	Microsoft Corporation
[+] RuntimeBroker.exe		2,880 K	15,320 K	775	Runtime Broker	Microsoft Corporation
[+] RuntimeBroker.exe		1,480 K	7,140 K	1045	Runtime Broker	Microsoft Corporation
[+] SecurityCenter.exe	0.25	100,136 K	30,044 K	392		
[+] smss.exe		9,124 K	27,180 K	1254	Windows Defender SmallSc...	Microsoft Corporation
[+] WinVistaSE.exe		2,228 K	9,280 K	11216		
[+] WinVistaSE.exe		3,360 K	10,636 K	1632		
[+] RuntimeBroker.exe		3,320 K	17,676 K	1989	Runtime Broker	Microsoft Corporation
[+] shost.exe	<0.01	7,296 K	14,240 K	1044	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe	<0.01	2,636 K	8,256 K	1054	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		1,292 K	4,888 K	1276	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		2,272 K	9,720 K	1416	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		2,136 K	12,688 K	1454	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		6,688 K	15,096 K	1492	Host Processes for Windows S...	Microsoft Corporation
[+] csrss.exe	<0.01	10,032 K	20,020 K	5980	Host Processes for Windows T...	Microsoft Corporation
[+] MSBuildRunner.exe	0.13	15,524 K	8,532 K	5982		
[+] shost.exe		1,532 K	5,236 K	1544	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		5,020 K	7,596 K	1654	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		4,784 K	13,076 K	1764	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		2,436 K	9,708 K	1776	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		3,176 K	12,250 K	1796	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		3,212 K	11,084 K	1884	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe	<0.01	7,884 K	41,112 K	5080	Shell Infrastructure Host	Microsoft Corporation
[+] Messenger.exe	0.25	299,280 K	276,744 K	10464	Messenger	Facebook Inc.
[+] csrss.exe		1,360 K	5,744 K	10466		
[+] shost.exe		1,596 K	5,916 K	1894	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		3,620 K	7,768 K	1956	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		2,544 K	7,320 K	2156	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		2,920 K	7,380 K	2288	Host Processes for Windows S...	Microsoft Corporation
[+] shost.exe		1,320 K	5,976 K	2330	Host Processes for Windows S...	Microsoft Corporation
[+] NVIDIA Container exe		5,252 K	18,200 K	2388	NVIDIA Container	NVIDIA Corporation

CPU Usage: 1.39% Commit Charge: 53.62% Processes: 188 Physical Usage: 56.84%

Task Manager Taskbar Navigation Icons: File Explorer, Edge, Chrome, Firefox, VLC media player, Spotify, Discord, Steam, GeForce Experience, NVIDIA Control Panel, AMD Radeon Software, Intel Graphics Command Center, Logitech G Hub, Corsair iCUE, ASUS Armoury Crate, MSI Dragon Center, Gigabyte Control Center, ASRock DeskMini Utility, AIDA64 Extreme, HWMonitor, CPU-Z, Speccy, CrystalDiskInfo, MiniTool Partition Manager, EaseUS Data Recovery Wizard, Recuva, CCleaner, Malwarebytes Anti-Malware, Avast Free Antivirus, AVG Free Antivirus, McAfee LiveSafe, Norton Security Scan, Bitdefender Internet Security, ESET NOD32 Antivirus, Kaspersky Security Cloud Free, Trend Micro HouseCall, Symantec Endpoint Protection, Sophos Home, Avira Free Antivirus, Comodo Firewall, ZoneAlarm Free Firewall, Netgear Armor, Linksys WRT56GL v2 Firmware, Asus RT-AX58U v1 Firmware, TP-LINK Archer AX55 v1 Firmware, Xiaomi Mi Router 4 Pro v2.0.0 Firmware, Huawei B535-20A v1.0.0 Firmware, Zte MF880T v1.0.0 Firmware, Htc Desire 20 lite v1.0.0 Firmware, Samsung Galaxy S20 FE 5G v1.0.0 Firmware, Google Pixel 4 XL v1.0.0 Firmware, Apple iPhone 11 Pro Max v1.0.0 Firmware, Sony Xperia 1 II v1.0.0 Firmware, LG Velvet v1.0.0 Firmware, Motorola Moto G Stylus v1.0.0 Firmware, OnePlus 8 Pro v1.0.0 Firmware, Vivo X60 Pro v1.0.0 Firmware, Oppo Reno6 Pro v1.0.0 Firmware, Realme GT Neo2 v1.0.0 Firmware, Nothing Phone 1 v1.0.0 Firmware, Fairphone 3 v1.0.0 Firmware, PinePhone Pro v1.0.0 Firmware, Librem 5 v1.0.0 Firmware, PuriOS v1.0.0 Firmware, GrapheneOS v1.0

Process Monitor - SystemTools

File Edit Event Filter Tools Options Help

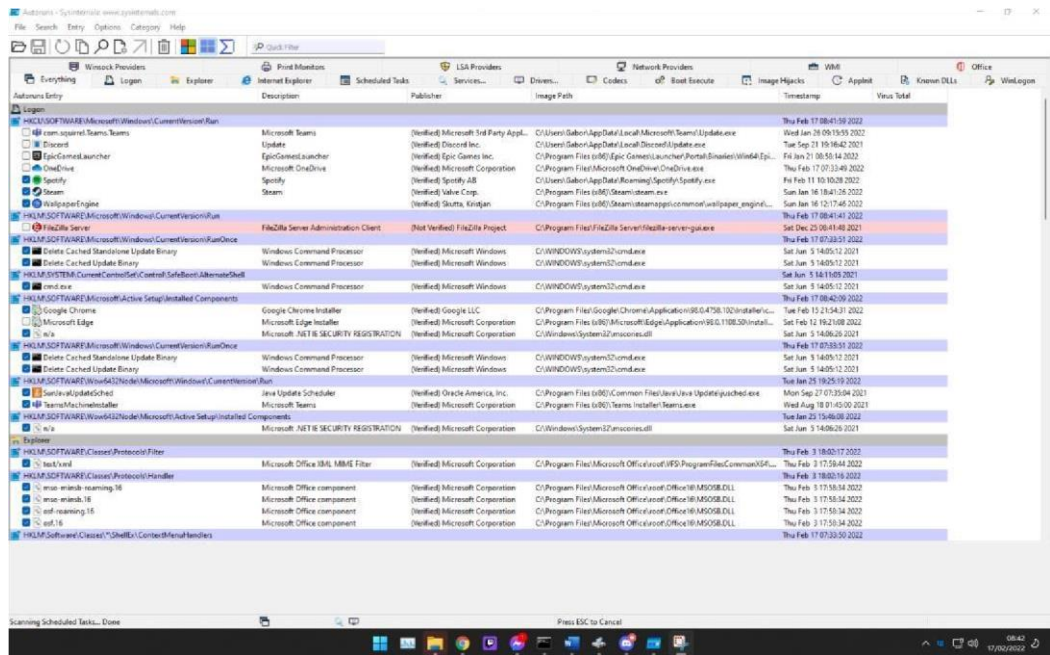
Time Process Name PID Operation Path Result Detail

00:00	svchost.exe	2500	Wt	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 3,170,304.
00:00	svchost.exe	2500	Wt	C:\Windows\System32\StateRepository	SUCCESS	Offset: 758,512. Le
00:00	svchost.exe	2500	Wt	C:\Windows\System32\StateRepository	SUCCESS	Offset: 692,224. Le
00:00	base.exe	564	Wt	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 3,149,824.
00:00	svchost.exe	2500	Wt	C:\Windows\System32\StateRepository	SUCCESS	Offset: 647,168. Le
00:00	MailEng.exe	3400	Wt	C:\Windows\System32\usb.dll	SUCCESS	Offset: 1,421,312.
00:00	MailEng.exe	3400	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 1,705,808.
00:00	base.exe	564	Wt	C:\Windows\System32\lsassr.dll	SUCCESS	Offset: 1,495,040.
00:00	svchost.exe	2500	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Exclusive: Fake O.
00:00	svchost.exe	2500	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 4,563,456.
00:00	MailEng.exe	3400	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 15,593,472.
00:00	svchost.exe	2500	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 121. Length:
00:00	MailEng.exe	3400	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 999,424. Le
00:00	base.exe	564	Wt	C:\Windows\System32\lsassr.dll	SUCCESS	Offset: 1,478,608.
00:00	svchost.exe	2500	RegOpenKey	HKLM\Software\Policies\Microsoft\MSI	NAME NOT FOUND	Denied Access: R.
00:00	svchost.exe	2500	RegOpenKey	HKU\S-1-5-18	REPAIR	Denied Access: M.
00:00	svchost.exe	2500	RegOpenKey	HKU\DEFAULT	SUCCESS	Denied Access: M.
00:00	svchost.exe	3400	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 15,577,088.
00:00	Explore.exe	6176	Wt	C:\Windows\System32\GDI.exe	SUCCESS	Offset: 802,816. Le
00:00	svchost.exe	2500	RegOpenKey	HKU\DEFAULT\Software\Policies\MSI	NAME NOT FOUND	Denied Access: R.
00:00	svchost.exe	2500	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop	SUCCESS	Denied Access: R.
00:00	svchost.exe	2500	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop	NAME NOT FOUND	Length: 12
00:00	svchost.exe	2500	RegOpenKey	HKU\DEFAULT	SUCCESS	
00:00	svchost.exe	2500	RegOpenKey	HKLM\Software\Policies\Microsoft\MSI	NAME NOT FOUND	Denied Access: R.
00:00	MailEng.exe	3400	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 3,193,328.
00:00	svchost.exe	2500	RegOpenKey	HKU\S-1-5-18	REPAIR	Denied Access: M.
00:00	svchost.exe	2500	RegOpenKey	HKU\DEFAULT	SUCCESS	Denied Access: M.
00:00	svchost.exe	2500	RegOpenKey	HKU\DEFAULT\Software\Policies\MSI	NAME NOT FOUND	Denied Access: R.
00:00	base.exe	564	Wt	C:\Windows\System32\lsassr.dll	SUCCESS	Offset: 1,392,640.
00:00	svchost.exe	2500	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop	NAME NOT FOUND	Denied Access: R.
00:00	svchost.exe	2500	RegOpenKey	HKU\DEFAULT	SUCCESS	
00:00	MailEng.exe	3400	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 15,581,472.
00:00	Explore.exe	6176	Wt	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2,226,432.
00:00	svchost.exe	2500	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Exclusive: Fake O.
00:00	svchost.exe	2500	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 121. Length:
00:00	MailEng.exe	3400	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 2,961,408.
00:00	base.exe	564	Wt	F:\SystemTools\SafePromoted.exe	SUCCESS	Query Name:
00:00	base.exe	564	Wt	F:\SystemTools\SafePromoted.exe	SUCCESS	Query Name:
00:00	MailEng.exe	3400	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 15,732,736.
00:00	Explore.exe	6176	Wt	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2,226,208.
00:00	MailEng.exe	3400	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 14,946,304.
00:00	MailEng.exe	3400	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 1,526,224.
00:00	Explore.exe	6176	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Name:
00:00	svchost.exe	2500	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Exclusive: Fake O.
00:00	Explore.exe	6176	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Name:
00:00	Explore.exe	6176	RegOpenKey	HKCU\Software\Classes\Applink.dll	NAME NOT FOUND	Denied Access: R.
00:00	svchost.exe	2500	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 121. Length:
00:00	Explore.exe	6176	RegOpenKey	HKCR\Applications\Promoted.exe	NAME NOT FOUND	Denied Access: R.
00:00	Explore.exe	6176	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Name:
00:00	Explore.exe	6176	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Name:
00:00	MailEng.exe	3400	Wt	F:\SystemTools\SafePromoted.exe	SUCCESS	Offset: 524,288. Le
00:00	Explore.exe	6176	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Name:
00:00	svchost.exe	2500	Wt	C:\ProgramData\Microsoft\Windows A	SUCCESS	Offset: 3,184,448.
00:00	MailEng.exe	3400	Wt	HKCR\Applications\Promoted.exe	NAME NOT FOUND	Denied Access: R.
00:00	Explore.exe	6176	Wt	F:\SystemTools\SafePromoted.exe	SUCCESS	Creation Time: 16:0.

Showing 284,699 of 600,175 events (47%)

Backed by virtual memory

17/02/2024 08:30



d)

Security Utilities

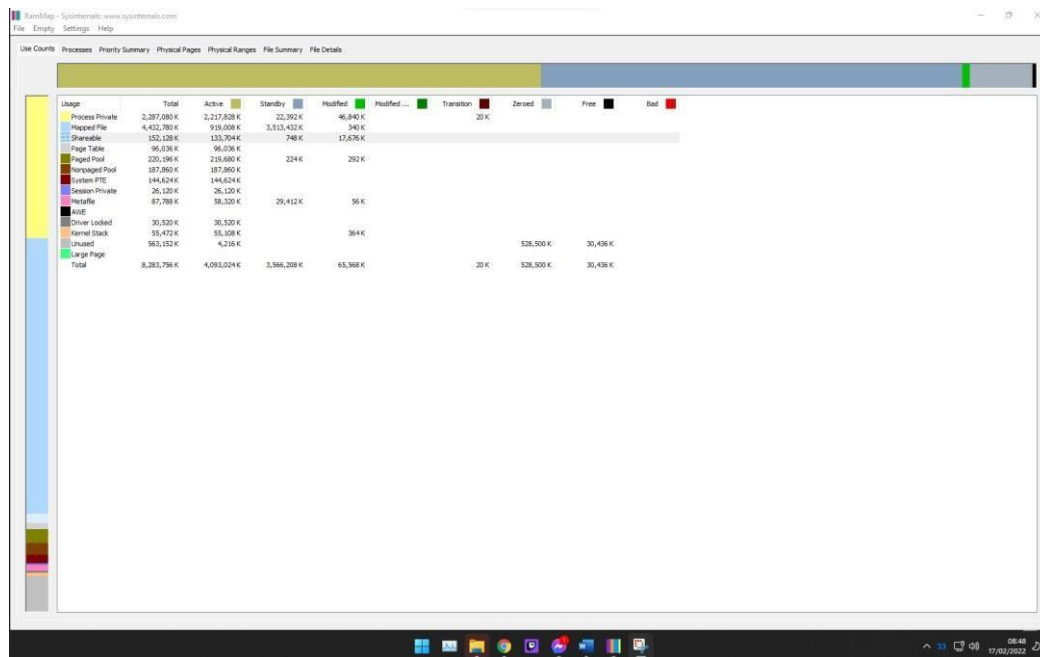
Logon session Szöveges lenyomatot készít arról mi mikor ki által történt , ezáltal visszakövethető bármilyen probléma esetén ki a hibás.

```
Shell
C:\>logonsessions -p

[13] Logon session 00000000:6a6d6160:
  User name:      NTDEV\markruss
  Auth package:   Kerberos
  Logon type:     RemoteInteractive
  Session:        1
  Sid:            S-1-5-21-397955417-626881126-188441444-3615555
  Logon time:     7/2/2015 6:05:31 PM
  Logon server:   NTDEV-99
  DNS Domain:    NTDEV.CORP.MICROSOFT.COM
  UPN:            markruss@ntdev.microsoft.com
  15368: ProcExp.exe
  17528: ProcExp64.exe
  13116: cmd.exe
  17100: conhost.exe
  6716: logonsessions.exe
```

e) Information Utilities

RaMMMap megmutatja hogy a windows hogy rendeli hozzá a memóriát a folyamatokhoz, mennyi fájl van a gyorsítótárakban illetve mi mennyi memóriát használ



3. Töltse le a következő programot: Dependency Walker

- a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dllből (Win alrendszer DLL)!

A program vagy utasításkészletéhez biztosít hozzáférést az API . Hívásoknál muszáj a content-type értéket megadni, xml formátumban kapja meg az alkalmazás.

Dependency Walker (VS2010)

File Edit View Options Profile Window Help

VS2010.DLL

KERNEL32.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL

NTDLL.DLL

KERNELBASE.DLL

API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL

EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL

EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL

EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL

EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-SIDEVIEW-L1-1-0.DLL

EXT-MS-WIN-MRM-CORER-RESMANAGER-L1-1-0.DLL

EXT-MS-WIN-NTDSAP-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL

EXT-MS-WIN-NTDSAP-ACTIVEDIRECTORYCLIENT-L1-1-1.DLL

EXT-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL

EXT-MS-WIN-SECURITY-NTMATH-L1-1-0.DLL

EXT-MS-WIN-SECURITY-CAPABILITY-L1-1-0.DLL

EXT-MS-WIN-SECURITY-EXPERIMENTAL-L1-1-0.DLL

Module

File Time Stamp

Link Time Stamp

File Size

Attr

Link Checksum

Real Checksum

CPU

Subsystem

Symbols

Preferred Base

Actual Base

Virtual Size

Load Order

File Ver

Error: At least one required implicit or forwarded dependency was not found.
 Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.
 Error: Modules with different CPU types were found.
 Warning: At least one delay-load dependency module was not found.

For Help, press F1

b.) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról! „

Windows kernel funkciókat tartalmaz, adatok olvasását és írását végzni, illetve ezáltal memóriát is kezel valamilyen szinten.

Dependency Walker (VS2010)

File Edit View Options Profile Window Help

VS2010.DLL

KERNEL32.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL

NTDLL.DLL

KERNELBASE.DLL

API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL

EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL

EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL

EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL

EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL

EXT-MS-WIN-KERNEL32-SIDEVIEW-L1-1-0.DLL

EXT-MS-WIN-MRM-CORER-RESMANAGER-L1-1-0.DLL

EXT-MS-WIN-NTDSAP-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL

EXT-MS-WIN-NTDSAP-ACTIVEDIRECTORYCLIENT-L1-1-1.DLL

EXT-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL

EXT-MS-WIN-SECURITY-NTMATH-L1-1-0.DLL

EXT-MS-WIN-SECURITY-CAPABILITY-L1-1-0.DLL

EXT-MS-WIN-SECURITY-EXPERIMENTAL-L1-1-0.DLL

Module

File Time Stamp

Link Time Stamp

File Size

Attr

Link Checksum

Real Checksum

CPU

Subsystem

Symbols

Preferred Base

Actual Base

Virtual Size

Load Order

File Ver

Error: At least one required implicit or forwarded dependency was not found.
 Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.
 Error: Modules with different CPU types were found.
 Warning: At least one delay-load dependency module was not found.

For Help, press F1