

# **Operációs rendszerek BSc**

**1. Gyak.**

**2022. 02. 17.**

**Készítette:**

**Szendrei GáborBsc**

**Programtervező informatikus**

**V9ZK10**

**Miskolc, 2022**

## 1. feladat

**a) Hozza létre a következő mappa szerkezetet!**

[illegible]

**b) Készítsen másolatot:**

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

```

C:\Users\user> cd C:\Users\user\Documents\Vegetim\Oprenszer\WVDC38
C:\Users\user\Documents\Vegetim\Oprenszer\WVDC38> copy land fa /e /t
C:\Users\user\Documents\Vegetim\Oprenszer\WVDC38> tree
Folder PATH listing
Volume serial number is 7EC9-6498
.
..
--bakor
--basan
--berack
--mgyoro
fa
--korte
--leder
land
--kokusz
--leder
C:\Users\user\Documents\Vegetim\Oprenszer\WVDC38>

```

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

The screenshot shows a Windows Command Prompt window with the following text:

```

C:\Users\user> cd /d "E:\Vegyetke\Oprendszerek\V92K3"
E:\Vegyetke\Oprendszerek\V92K3> copy bokor fa /E /T
E:\Vegyetke\Oprendszerek\V92K3> tree
Folder PATH listing
Volume serial number is 7EC9-6498
.
..
bokor
  banan
  barack
  meggyora
fa
  banan
  barack
  szeder
janc
  bokusz
  szeder
E:\Vegyetke\Oprendszerek\V92K3>

```

The taskbar at the bottom shows the date and time as 08:03 17/02/2022.

**c) Végezze el a következő áthelyezéseket:**

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

```
C:\Windows\system32\cmd.exe
E:\legyetem\oprendszer\V9ZX18>move boker\barack fa
1 dir(s) moved.

E:\legyetem\oprendszer\V9ZX18>tree
Folder PATH listing
Volume serial number is 7EC9-649B
.
..
boker
|_ banan
|_ egygyoro
fa
|_ banan
|_ barack
|_ korte
|_ zeder
land
|_ kokusz
|_ zieder

E:\legyetem\oprendszer\V9ZX18>
```

- 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
.
.
.
--bokor
|   --banan
|   --mogoroso
|   --fa
|       --banan
|       --barack
|       --kokusz
|       --korte
|       --szeder
--land
    --szeder
E:\legyetem\Oprendszer\V92K18>
```

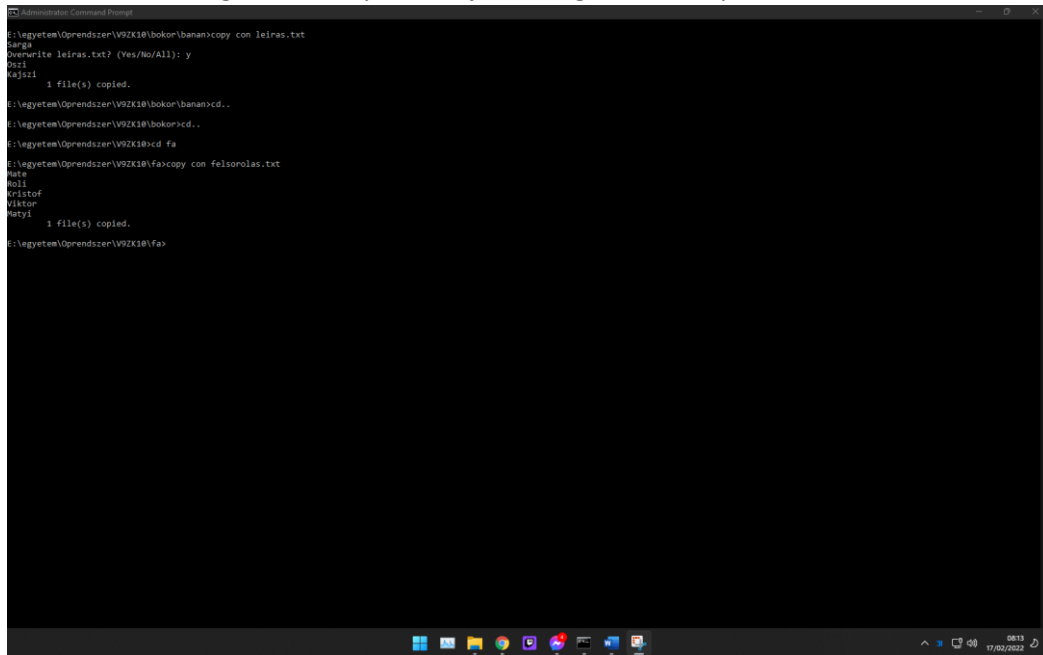
d) Törölje a neptunkod/land katalógust a teljes tartalmával.  
Hozza létre a következő szöveges állományokat:

- 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
.
.
.
--bokor
|   --banan
|   --mogoroso
|   --fa
|       --banan
|       --barack
|       --kokusz
|       --korte
|       --szeder
--land
    --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.txt
E:\legyetem\Oprendszer\V92K18\fa>
```

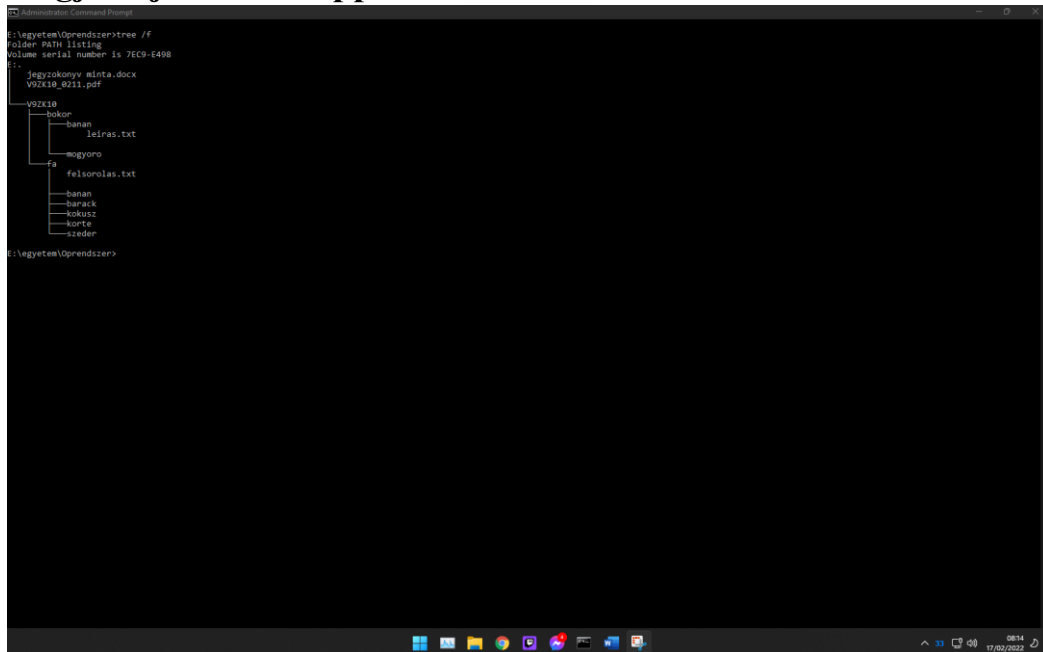
**e) A leiras.txt szöveges állományba írjon 3 sort a barackról.**

A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét.



```
Administrator: Command Prompt
E:\egyetem\Oprendszer\V92K10\bokor\banan>copy con leiras.txt
leira
Overwrite leiras.txt? (Yes/No/All): y
Dsc1
Hajsz1
1 file(s) copied.
E:\egyetem\Oprendszer\V92K10\bokor\banan>cd..
E:\egyetem\Oprendszer\V92K10\bokor>cd..
E:\egyetem\Oprendszer\V92K10>cd fa
E:\egyetem\Oprendszer\V92K10\fa>copy con felsorolas.txt
Rene
Pall
Krisztof
Viktor
Matyi
1 file(s) copied.
E:\egyetem\Oprendszer\V92K10\fa>
```

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



```
Administrator: Command Prompt
E:\egyetem\Oprendszer>tree /f
Folder Path listing
Volume serial number is 7EC9-6408
.
.
jegyzokonyv_minta.docx
V92K10_0211.pdf
V92K10
├── bokor
│   ├── banan
│   └── leiras.txt
├── egyono
└── fa
    ├── felsorolas.txt
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder
E:\egyetem\Oprendszer>
```

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

```
Administrator: Command Prompt
E:\egyetem\oprendszer\V92K18>dir /S /e*
Volume in drive E has no label.
Volume Serial Number is 7EC9-E498

Directory of E:\egyetem\oprendszer\V92K18\borok\banan
17/02/2022  08:12                21 leiras.txt
               1 File(s)                21 bytes

Directory of E:\egyetem\oprendszer\V92K18\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:\egyetem\oprendszer\V92K18>
```

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

```
Administrator: Command Prompt
E:\egyetem\oprendszer\V92K18>cd fa
E:\egyetem\oprendszer\V92K18\fa>attrib +r felsorolas.txt
E:\egyetem\oprendszer\V92K18\fa>
```

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

```
Administration Command Prompt

Directory of E:\vegyetem\Oprendszer\V92K10\bokor\banan
17/02/2022 08:11 <DIR> .
17/02/2022 08:03 <DIR> ..
17/02/2022 08:12 21 l6dres.txt
1 File(s) 21 bytes

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

Directory of E:\vegyetem\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 38 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:\vegyetem\Oprendszer\V92K10\fa\banan
17/02/2022 07:48 <DIR> .
17/02/2022 08:13 <DIR> ..
0 File(s) 0 bytes

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

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

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

Directory of E:\vegyetem\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) 35,317,670,704 bytes free

E:\vegyetem\Oprendszer>
```

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

```
Administration Command Prompt

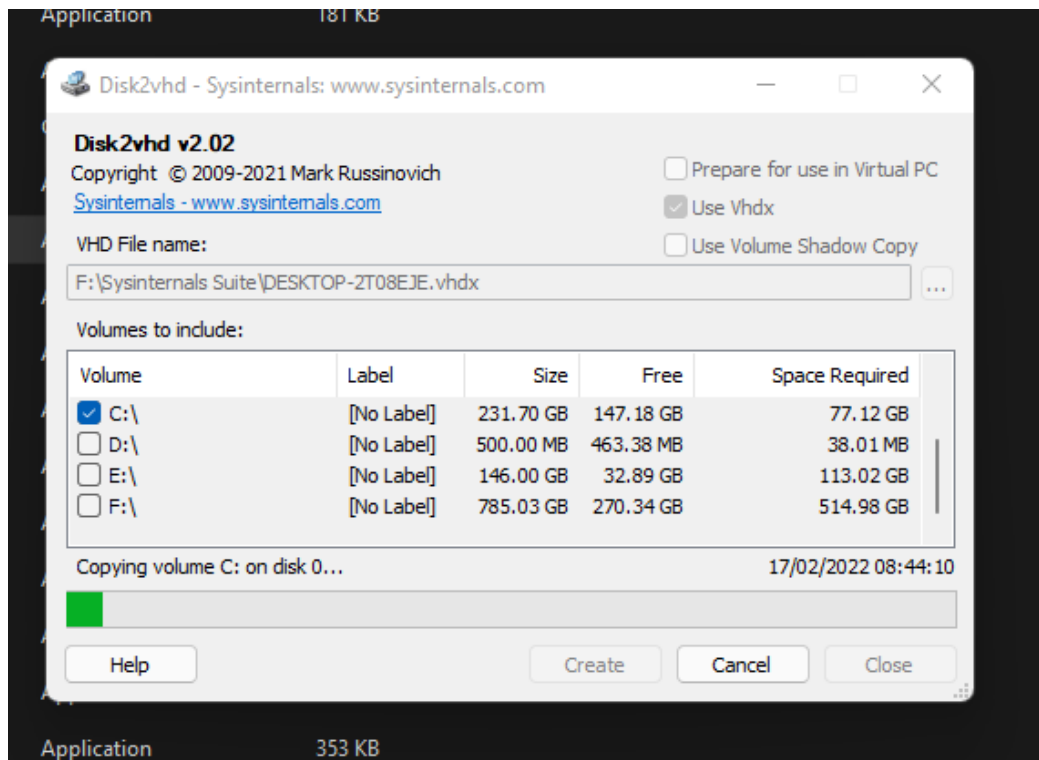
E:\vegyetem\Oprendszer\V92K10\fa>sort felsorolas.txt
Viktor
Pate
Petyl
Rusi
Viktor

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

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

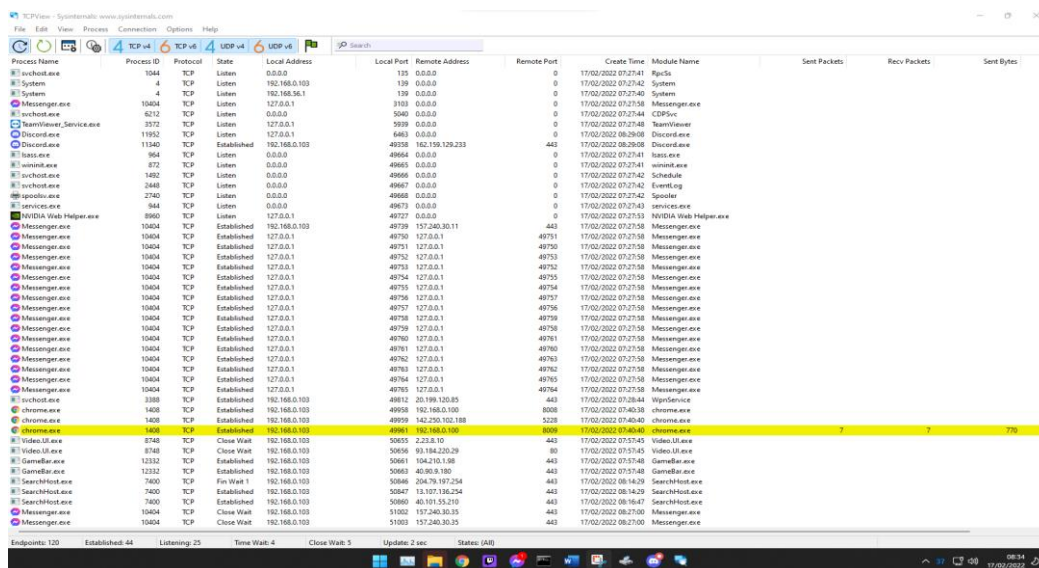
a) File and Disk Utilities (Disk2vhd)

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





### c) Process Utilities

A Process Explorer információkat jelenít meg arról, hogy mely leírók és DLL-ek folyamatai vannak megnyitva vagy futtatva.

[illegible]

A process monitor egy haladó monitorozó alkalmazás. Ami valós időben mutatja a fájlrendszert a regiszter és process aktivitásokat.

Process Monitor - SystemTools

www.systemtools.com

File Edit View Filter Tools Help

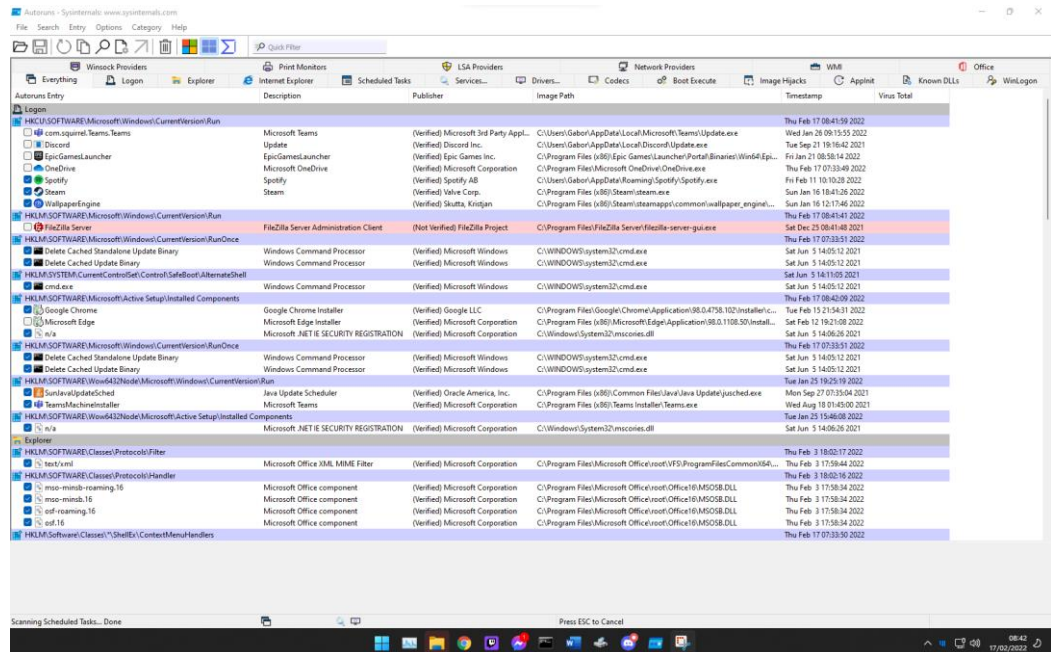
Time	Process Name	PID	Operation	Path	Result	Detail
00:30:	svchost.exe	2580	Io ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 3,170,304...
00:30:	svchost.exe	2580	Io ReadFile	C:\Windows\System32\SHELL32.dll	SUCCESS	Offset: 704,512...
00:30:	svchost.exe	2580	Io ReadFile	C:\Windows\System32\ShellExtFactory.dll	SUCCESS	Offset: 603,224...
00:30:	svchost.exe	2580	Io ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 3,143,624...
00:30:	svchost.exe	2580	Io ReadFile	C:\Windows\System32\SHELL32.dll	SUCCESS	Offset: 647,168...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\Windows\System32\Zwapi.dll	SUCCESS	Offset: 1,211,312...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows Da...	SUCCESS	Offset: 1,105,520...
00:30:	svchost.exe	2580	Io ReadFile	C:\Windows\System32\user.dll	SUCCESS	Offset: 1,495,040...
00:30:	svchost.exe	2580	Io Lock File	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Exclusive File O...
00:30:	svchost.exe	2580	Io ReadFile	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Offset: 4,953,456...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows Da...	SUCCESS	Offset: 15,593,472...
00:30:	svchost.exe	2580	Io Hooked Package	C:\ProgramData\Microsoft\Windows D...	SUCCESS	Offset: 123 Length...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows Da...	SUCCESS	Offset: 399,424...
00:30:	svchost.exe	2580	Io ReadFile	C:\Windows\System32\user.dll	SUCCESS	Offset: 1,476,656...
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_LOCAL_MACHINE\Software\Palmco...MUI...	NAME NOT FOUND	Denied Access R...
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_5-1-S-18	REPAIRME	Denied Access R...
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_DEFAULT	SUCCESS	Denied Access R...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows Da...	SUCCESS	Offset: 15,577,208...
00:30:	svchost.exe	2580	Io Hooked Package	C:\Windows\System32\SHCore.dll	SUCCESS	Offset: 802,816...
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_DEFAULT\Software\Palmco...MUI...	NAME NOT FOUND	Denied Access R...
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_DEFAULT\Control Panel\Desktop	SUCCESS	Denied Access R...
00:30:	svchost.exe	2580	ProgOpenValue	HKEY_DEFAULT\Control Panel\Desktop	NAME NOT FOUND	Length 12
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_DEFAULT\Control Panel\Desktop	SUCCESS	
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_LOCAL_MACHINE\Software\Palmco...MUI...	NAME NOT FOUND	Denied Access R...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows D...	SUCCESS	Offset: 1,105,520...
00:30:	svchost.exe	2580	Io Hooked Package	C:\Windows\System32\user.dll	REPAIRME	Denied Access R...
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_DEFAULT	SUCCESS	Denied Access R...
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_DEFAULT\Software\Palmco...MUI...	NAME NOT FOUND	Denied Access R...
00:30:	svchost.exe	2580	Io ReadFile	C:\Windows\System32\user.dll	SUCCESS	Offset: 1,392,640...
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_DEFAULT\Control Panel\Desktop	NAME NOT FOUND	Denied Access R...
00:30:	svchost.exe	2580	ProgOpenKey	HKEY_DEFAULT	SUCCESS	
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows D...	SUCCESS	Offset: 15,601,472...
00:30:	svchost.exe	2580	Io Hooked Package	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2,226,688...
00:30:	svchost.exe	2580	Io Lock File	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Exclusive File O...
00:30:	svchost.exe	2580	Io Hooked Package	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Offset: 123 Length...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows D...	SUCCESS	Offset: 2,961,408...
00:30:	svchost.exe	2580	Io OpenNameSpace	F:\SystemRoot\System\Phonon04.exe	SUCCESS	
00:30:	svchost.exe	2580	Io OpenNameSpace	F:\SystemRoot\System\Phonon04.exe	SUCCESS	Name = Systemat...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows D...	SUCCESS	Offset: 17,732,736...
00:30:	svchost.exe	2580	Io Hooked Package	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2,206,208...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows D...	SUCCESS	Offset: 1,946,304...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows D...	SUCCESS	Offset: 1,536,256...
00:30:	Explore.exe	6176	ProgOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query Name...
00:30:	Explore.exe	6176	ProgOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query NameData...
00:30:	svchost.exe	2580	Io Lock File	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Exclusive File O...
00:30:	MkHKey.exe	3480	Io ReadFile	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query NameData...
00:30:	Explore.exe	6176	ProgOpenKey	HKEY_CURRENT_USER\Software\Classes\Applications...	NAME NOT FOUND	Denied Access R...
00:30:	svchost.exe	2580	Io Hooked Package	C:\ProgramData\Microsoft\Windows A...	SUCCESS	Offset: 123 Length...
00:30:	Explore.exe	6176	ProgOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query Name...
00:30:	Explore.exe	6176	ProgOpenKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query NameData...
00:30:	MkHKey.exe	3480	Io ReadFile	F:\SystemRoot\System\Phonon04.exe	SUCCESS	Offset: 524,288...
00:30:	svchost.exe	2580	Io Hooked Package	C:\Windows\System32\user.dll	SUCCESS	Query NameData...
00:30:	Explore.exe	6176	ProgOpenKey	HKEY_CURRENT_USER\Software\Classes\Applications...	NAME NOT FOUND	Denied Access R...
00:30:	MkHKey.exe	3480	Io ReadFile	C:\ProgramData\Microsoft\Windows D...	SUCCESS	Offset: 1,944,448...
00:30:	Explore.exe	6176	ProgOpenKey	HKEY_CURRENT_USER\Software\Classes	NAME NOT FOUND	Denied Access R...
00:30:	Explore.exe	6176	Io OpenOpen	F:\SystemRoot\System\Phonon04.exe	SUCCESS	Creation Time: 16:0...

Showing 284,699 of 603,575 events (47%)

Backed up by virtual memory

08:30  
17/02/2022

Autoruns-ban a windows indulásakor lefutó folyamatokat tudjuk szabályozni , letiltani, engedélyezni.



#### d) Security Utilities

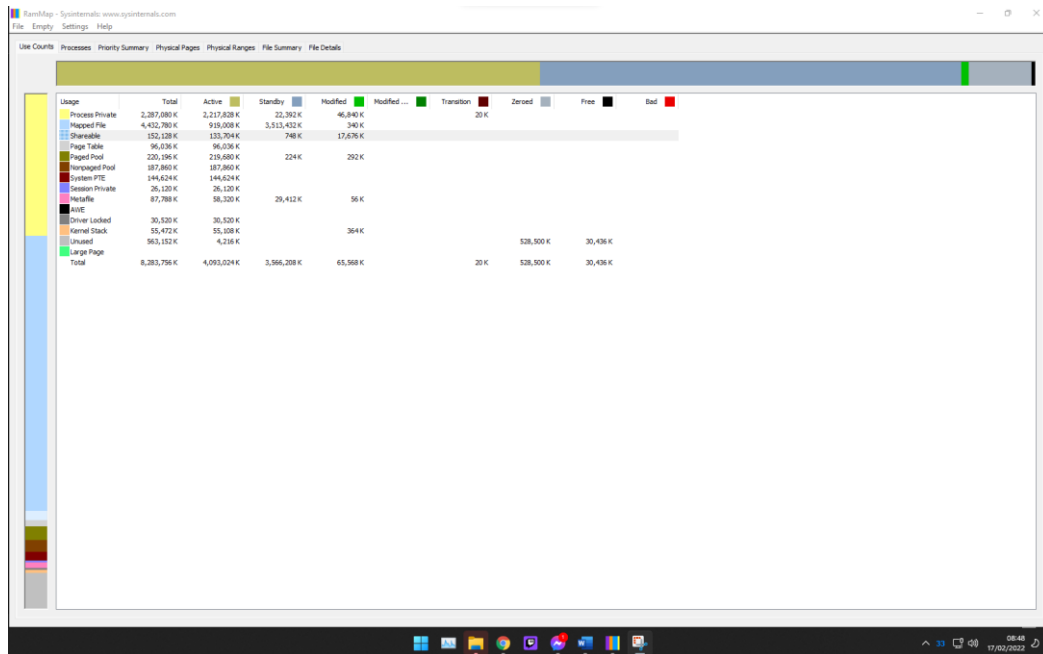
Login session Szöveges lenyomatot készít arról mi mikor ki által történt , ezáltal visszakövethető bármilyen probléma esetén ki a hibás.

```
Shell
C:\>logonsessions -p

[13] Login 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

RaMMap 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.dll-ből (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 (VSIX10)

Module List:

- kernel32.dll
- API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
- API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
- NTDLL.dll
- KERNELBASE.dll
- NTDLL.dll
- API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
- EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
- EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
- EXT-MS-WIN-NTUSER-SHELL-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-QUICKS-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-SIDEBYSE-L1-1-0.DLL
- EXT-MS-WIN-MINICORER-RESMANAGER-L1-1-0.DLL
- EXT-MS-WIN-GAPI-GROUPPOLICY-L1-1-0.DLL
- EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL
- EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL
- EXT-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL
- EXT-MS-WIN-ADVAPI32-NTMART-L1-1-0.DLL
- EXT-MS-WIN-SECURITY-CAPAUTHZ-L1-1-1-0.DLL
- EXT-MS-WIN-SECURITY-CAPAUTHZ-L1-1-1-0.DLL

Function List:

Ordinal	Hint	Function	Entry Point
N/A	289 (0x0110)	DllMain	Not Bound
N/A	305 (0x0111)	EnterCriticalSection	Not Bound
N/A	536 (0x0218)	GetCurrentProcess	Not Bound
N/A	537 (0x0219)	GetCurrentProcessId	Not Bound
N/A	541 (0x0210)	GetCurrentThreadId	Not Bound
N/A	610 (0x0242)	GetLastError	Not Bound
N/A	722 (0x02D0)	GetStartupInfoA	Not Bound
N/A	747 (0x02E8)	GetSystemTimeAsFileTime	Not Bound
N/A	775 (0x0317)	GetTickCount	Not Bound
N/A	864 (0x0360)	InitializeCriticalSection	Not Bound
N/A	952 (0x0388)	LeaveCriticalSection	Not Bound
N/A	1084 (0x0446)	QueryPerformanceCounter	Not Bound
N/A	1180 (0x049C)	RtlAddFunctionTable	Not Bound

Link Checksum: 0x00000000

Module List (continued):

Module	File Time Stamp	Link Time Stamp	File Size	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	File Ver
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-COMMA-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).												
API-MS-WIN-CORE-DATETIME-L1-2-0.DLL	Error opening file. The system cannot find the file specified (2).												

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.

- 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 - [VSXCLXE]

VSXCLXE

Kernel32.dll

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

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

NTDLL.dll

KernelBase.dll

NTDLL.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-KERNEL32-FILE-L1-1-0.DLL

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

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

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

EXT-MS-WIN-MRMACORER-REMANAGER-L1-1-0.DLL

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

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

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

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

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

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

Pi	Ordinal	Hint	Function	Entry Point
N/A	18 (0x0112)		ApiSetQueryApiSetPresence	Not Bound
N/A	20 (0x014)		CurllocateCapturedBuffer	Not Bound
N/A	21 (0x015)		CurllocateMessagePointer	Not Bound
N/A	26 (0x01A)		CurllocateCallServer	Not Bound
N/A	28 (0x01C)		CurllocateCaptureBuffer	Not Bound
N/A	32 (0x020)		CurllocateRegion	Not Bound
N/A	34 (0x022)		CurlPrint	Not Bound
N/A	35 (0x023)		CurlPrintEx	Not Bound
N/A	45 (0x02D)		DebugThreadDebugObject	Not Bound
N/A	46 (0x02E)		DebugThreadDebugObjectEx	Not Bound
N/A	57 (0x039)		EndEventEnabled	Not Bound
N/A	59 (0x03B)		EndEventRegister	Not Bound
N/A	61 (0x03D)		EndEventUnregister	Not Bound

Pi	Ordinal	Hint	Function	Entry Point
8 (0x0008)	534 (0x346)		RtlDispatchAPC	0x0002A140
9 (0x0009)	723 (0x2D3)		RtlActivateActivationContextUnsafeFast	0x0003F240
10 (0x000A)	891 (0x37B)		RtlDeactivateActivationContextUnsafeFast	0x0003F380
11 (0x000B)	1185 (0x4A1)		RtlInterlockedPushList	0x000C2700
12 (0x000C)	1534 (0x5FE)		RtlInterlockedPushListEx	0x000C2780
13 (0x000D)	1533 (0x5FD)		RtlInterlockedPushListEx2	0x000C27C0
14 (0x000E)	1579 (0x62B)		RtlInterlockedPushListEx3	0x000C27E0
15 (0x000F)	0 (0x000)		A_SdkFinal	0x0008A8E0
16 (0x0010)	1 (0x001)		A_SdkInit	0x0008A900
17 (0x0011)	2 (0x002)		A_SdkUpdate	0x0008A960
18 (0x0012)	3 (0x003)		AlpAdjustCompletionListConcurrencyCount	0x000C27F0
19 (0x0013)	4 (0x004)		AlpFreeCompletionListMessage	0x000C2820

Module	File Time Stamp	Link Time Stamp	File Size	Abn.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	File Ver
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-COMBA1-1-0.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-CONSOLE-L2-0.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-CONSOLE-L2-1.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-CONSOLE-L2-2.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-CONSOLE-L3-0.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-CONSOLE-L3-1.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-CONSOLE-L3-2.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-DATETIME-L1-1-1.DLL	Error opening file. The system cannot find the file specified (2).													
API-MS-WIN-CORE-DATETIME-L1-1-2.DLL	Error opening file. The system cannot find the file specified (2).													

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