

# **Operációs rendszerek BSc**

**2. Gyak.**

**2022. 02. 16.**

**Készítette:**

Pázmán András Bsc

Szak Mérnökinformatikus

Neptunkód H2Z4X3

**Miskolc, 2022**

## Feladatok

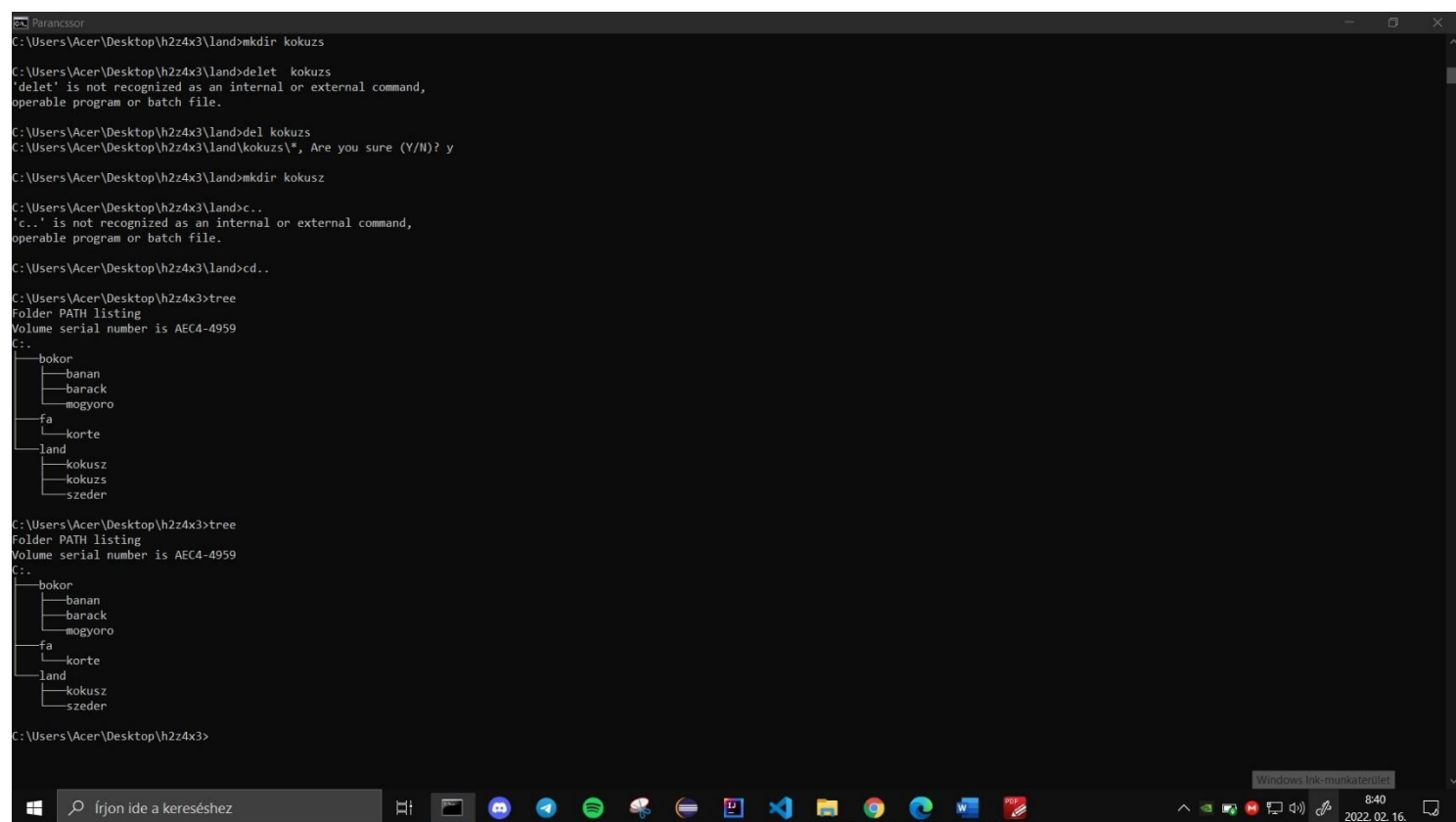
1. Készítse el a következő feladatokat! **Mentés:** Írja le a program szolgáltatásait és a futtatás eredményét a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).

Az elvégzett feladatokról készítsen (a.)-j.)-ig.) képernyőképet, majd illessze be a jegyzőkönyvbe.

a.) Hozza létre a következő mappa szerkezetet!

neptunkod

```
|
|- bokor
|   |- banan
|   |- mogyoro
|   |- barack
|
|- fa
|   |- korte
|
|-land
    |- szeder
    |- kokusz
```



```
cs Parancssor
C:\Users\Acer\Desktop\h2z4x3\land>mkdir kokuzs
C:\Users\Acer\Desktop\h2z4x3\land>delet kokuzs
'delet' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Acer\Desktop\h2z4x3\land>del kokuzs
C:\Users\Acer\Desktop\h2z4x3\land>kokuzs\*, Are you sure (Y/N)? y
C:\Users\Acer\Desktop\h2z4x3\land>mkdir kokusz
C:\Users\Acer\Desktop\h2z4x3\land>c..
'c..' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Acer\Desktop\h2z4x3\land>cd..
C:\Users\Acer\Desktop\h2z4x3>tree
Folder PATH listing
Volume serial number is AEC4-4959
C:.
|-- bokor
|   |-- banan
|   |-- barack
|   |-- mogyoro
|-- fa
|   |-- korte
|-- land
|   |-- kokusz
|   |-- kokuzs
|   |-- szeder
C:\Users\Acer\Desktop\h2z4x3>tree
Folder PATH listing
Volume serial number is AEC4-4959
C:.
|-- bokor
|   |-- banan
|   |-- barack
|   |-- mogyoro
|-- fa
|   |-- korte
|-- land
|   |-- kokusz
|   |-- kokuzs
|   |-- szeder
C:\Users\Acer\Desktop\h2z4x3>
```

b.) Készítsen másolatot:

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

```
Parancssor

C:\Users\Acer\Desktop\h2z4x3>tree
Folder PATH listing
Volume serial number is AEC4-4959
C:.
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   ├── korte
│   └── szeder
├── land
│   ├── kokusz
│   └── szeder
└── 
```

C:\Users\Acer\Desktop\h2z4x3>

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

```
Parancssor

Directory of C:\Users\Acer\Desktop\h2z4x3
2022. 02. 16. 08:34 <DIR>      .
2022. 02. 16. 08:34 <DIR>      ..
2022. 02. 16. 08:47 <DIR>      bokor
2022. 02. 16. 08:48 <DIR>      fa
2022. 02. 16. 08:48 <DIR>      land
                0 File(s)      0 bytes
                5 Dir(s)  23 783 776 256 bytes free

C:\Users\Acer\Desktop\h2z4x3>tree
Folder PATH listing
Volume serial number is AEC4-4959
C:.
├── bokor
│   ├── banan
│   ├── mogyoro
│   └── 
```

C:\Users\Acer\Desktop\h2z4x3>

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

állományokat: • *neptunkod/bokor/banan/leiras.txt*

• *neptunkod/tree/felsorolas.txt*

```
2022. 02. 16. 08:55 <DIR> ..
2022. 02. 16. 08:55 0 leiras.txt.txt
1 File(s) 0 bytes
2 Dir(s) 23 775 330 304 bytes free

C:\Users\Acer\Desktop\h2z4x3\bokor\banan>dir
Volume in drive C has no label.
Volume Serial Number is AEC4-4959

Directory of C:\Users\Acer\Desktop\h2z4x3\bokor\banan

2022. 02. 16. 08:57 <DIR> .
2022. 02. 16. 08:57 <DIR> ..
2022. 02. 16. 08:57 0 leiras.txt
1 File(s) 0 bytes
2 Dir(s) 23 775 432 704 bytes free

C:\Users\Acer\Desktop\h2z4x3\bokor\banan>cd ..

C:\Users\Acer\Desktop\h2z4x3\bokor>cd ..

C:\Users\Acer\Desktop\h2z4x3>fa
'fa' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Acer\Desktop\h2z4x3>cd fa

C:\Users\Acer\Desktop\h2z4x3\fa>dir
Volume in drive C has no label.
Volume Serial Number is AEC4-4959

Directory of C:\Users\Acer\Desktop\h2z4x3\fa

2022. 02. 16. 08:56 <DIR> .
2022. 02. 16. 08:56 <DIR> ..
2022. 02. 16. 08:35 <DIR> barack
2022. 02. 16. 08:55 0 felsorolas.txt
2022. 02. 16. 08:39 <DIR> kokusz
2022. 02. 16. 08:38 <DIR> korte
2022. 02. 16. 08:38 <DIR> szeder
1 File(s) 0 bytes
6 Dir(s) 23 775 203 328 bytes free
```

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

A *felsorolas* szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

```
C:\Users\Acer\Desktop\h2z4x3\fa>dir
Volume in drive C has no label.
Volume Serial Number is AEC4-4959

Directory of C:\Users\Acer\Desktop\h2z4x3\fa

2022. 02. 16. 09:02 <DIR> .
2022. 02. 16. 09:02 <DIR> ..
2022. 02. 16. 08:35 <DIR> barack
2022. 02. 16. 09:00 35 felsorolas.txt
2022. 02. 16. 08:39 <DIR> kokusz
2022. 02. 16. 08:38 <DIR> korte
2022. 02. 16. 08:38 <DIR> szeder
1 File(s) 35 bytes
6 Dir(s) 23 784 468 480 bytes free

C:\Users\Acer\Desktop\h2z4x3\fa>cd felsorolas.txt
Érvénytelen a könyvtárnév.

C:\Users\Acer\Desktop\h2z4x3\fa>
C:\Users\Acer\Desktop\h2z4x3\fa>
```

felsorolas - Jegyzetfőm

Fájl Szerkesztés Formátum Nézet Súgó

dani  
zoli  
kristof  
sanyi  
david

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

```

C:\Users\Acer\Desktop>dir /s
Volume in drive C has no label.
Volume Serial Number is AEC4-4959

Directory of C:\Users\Acer\Desktop\h2z4x3

2022. 02. 16. 08:34 <DIR>      .
2022. 02. 16. 08:34 <DIR>      ..
2022. 02. 16. 08:47 <DIR>      bokor
2022. 02. 16. 09:02 <DIR>      fa
2022. 02. 16. 08:48 <DIR>      land
0 File(s)              0 bytes

Directory of C:\Users\Acer\Desktop\h2z4x3\bokor

2022. 02. 16. 08:47 <DIR>      .
2022. 02. 16. 08:47 <DIR>      ..
2022. 02. 16. 08:57 <DIR>      banan
2022. 02. 16. 08:35 <DIR>      mogyoro
0 File(s)              0 bytes

Directory of C:\Users\Acer\Desktop\h2z4x3\bokor\banan

2022. 02. 16. 08:57 <DIR>      .
2022. 02. 16. 08:57 <DIR>      ..
2022. 02. 16. 08:59      50 leiras.txt
1 File(s)              50 bytes

Directory of C:\Users\Acer\Desktop\h2z4x3\bokor\mogyoro

2022. 02. 16. 08:35 <DIR>      .
2022. 02. 16. 08:35 <DIR>      ..

```

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

```

C:\Users\Acer\Desktop\h2z4x3>dir /s
Volume in drive C has no label.
Volume Serial Number is AEC4-4959

Directory of C:\Users\Acer\Desktop\h2z4x3\land\szeder

2022. 02. 16. 08:38 <DIR>      .
2022. 02. 16. 08:38 <DIR>      ..
0 File(s)              0 bytes

Total Files Listed:
2 File(s)              85 bytes
32 Dir(s) 23 779 962 880 bytes free

C:\Users\Acer\Desktop\h2z4x3>dir /s
Volume in drive C has no label.
Volume Serial Number is AEC4-4959

Directory of C:\Users\Acer\Desktop\h2z4x3\bokor\banan

2022. 02. 16. 08:59      50 leiras.txt
1 File(s)              50 bytes

Directory of C:\Users\Acer\Desktop\h2z4x3\fa

2022. 02. 16. 09:00      35 felsorolas.txt
1 File(s)              35 bytes

Total Files Listed:
2 File(s)              85 bytes
0 Dir(s) 23 782 072 320 bytes free

C:\Users\Acer\Desktop\h2z4x3>

```

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

```
Parancssor
2022. 02. 16. 08:38 <DIR>          szeder
0 File(s)          0 bytes

Directory of C:\Users\Acer\Desktop\h2z4x3\land\szeder
2022. 02. 16. 08:38 <DIR>          .
2022. 02. 16. 08:38 <DIR>          ..
0 File(s)          0 bytes

Total Files Listed:
2 File(s)          85 bytes
32 Dir(s) 23 779 962 880 bytes free

C:\Users\Acer\Desktop\h2z4x3>dir ?e*/s
Volume in drive C has no label.
Volume Serial Number is AEC4-4959

Directory of C:\Users\Acer\Desktop\h2z4x3\bokor\banan
2022. 02. 16. 08:59          50 leiras.txt
1 File(s)          50 bytes

Directory of C:\Users\Acer\Desktop\h2z4x3\fa
2022. 02. 16. 09:00          35 felsorolas.txt
1 File(s)          35 bytes

Total Files Listed:
2 File(s)          85 bytes
0 Dir(s) 23 782 072 320 bytes free

C:\Users\Acer\Desktop\h2z4x3>
```

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

```
Parancssor
Volume in drive C has no label.
Volume Serial Number is AEC4-4959

Directory of C:\Users\Acer\Desktop\h2z4x3\bokor\banan
2022. 02. 16. 08:59          50 leiras.txt
1 File(s)          50 bytes

Directory of C:\Users\Acer\Desktop\h2z4x3\fa
2022. 02. 16. 09:00          35 felsorolas.txt
1 File(s)          35 bytes

Total Files Listed:
2 File(s)          85 bytes
0 Dir(s) 23 782 072 320 bytes free

C:\Users\Acer\Desktop\h2z4x3>cd fa
C:\Users\Acer\Desktop\h2z4x3\fa>sort fa/felsorolas.txt /o /fa/felsorolass.txt
fa/felsorolas.txtA rendszer nem tal lja a megadott el'r'si utat.

C:\Users\Acer\Desktop\h2z4x3\fa>cd ..
C:\Users\Acer\Desktop\h2z4x3>sort fa/felsorolas.txt /o /fa/felsorolass.txt
/fa/felsorolass.txtA rendszer nem tal lja a megadott el'r'si utat.

C:\Users\Acer\Desktop\h2z4x3>cd fa
C:\Users\Acer\Desktop\h2z4x3\fa>sort felsorolas.txt /o felsorolass.txt
C:\Users\Acer\Desktop\h2z4x3\fa>type felsorolass.txt
dani
david
kristof
sanyi
zoli

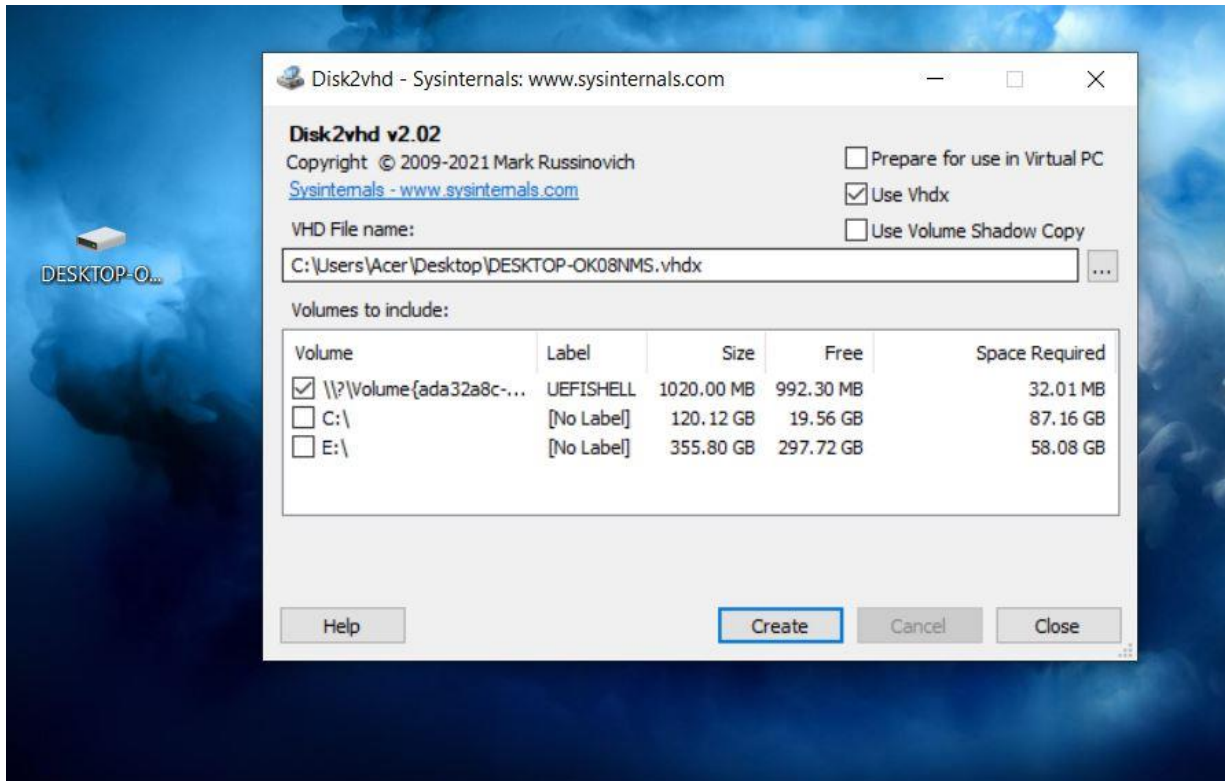
C:\Users\Acer\Desktop\h2z4x3\fa>
```

2. Tölts le a *Sysinternals Suite* csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít. <https://docs.microsoft.com/hu-hu/sysinternals/downloads/sysinternals-suite>

A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el:

A felsorolt eszközök közül minden eszköz esetén tölts 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 program egy virtuális másolatot készít a kijelölt lemezről



## b) Networking Utilities (TCPView)

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6

Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
MEGAsync.exe	16972	TCP	Established	172.18.2.161	57022	66.203.125.14	443	2022.02.16.15:02:12	MEGAsync.exe
svchost.exe	4464	TCP	Established	172.18.2.161	58441	20.199.120.182	443	2022.02.16.13:30:49	WpnService
NVIDIA Web Helper.exe	1124	TCP	Established	127.0.0.1	58443	127.0.0.1	58478	2022.02.16.13:30:54	NVIDIA Web Hel
NVIDIA Web Helper.exe	1124	TCP	Listen	127.0.0.1	58443	0.0.0.0	0	2022.02.16.13:30:51	NVIDIA Web Hel
NVIDIA Share.exe	9468	TCP	Established	127.0.0.1	58478	127.0.0.1	58443	2022.02.16.13:30:54	NVIDIA Share.exe
nvcontainer.exe	15152	TCP	Established	127.0.0.1	62417	127.0.0.1	65001	2022.02.16.13:30:42	nvcontainer.exe
nvcontainer.exe	15152	TCP	Established	127.0.0.1	65001	127.0.0.1	62417	2022.02.16.13:30:42	nvcontainer.exe
nvcontainer.exe	15152	TCP	Listen	127.0.0.1	65001	0.0.0.0	0	2022.02.14.22:09:44	nvcontainer.exe
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	2022.02.11.9:32:19	System
svchost.exe	14508	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	2022.02.16.13:30:40	DoSvc
svchost.exe	1064	TCPv6	Listen	::	135	::	0	2022.02.11.9:32:18	RpcSs
System	4	TCPv6	Listen	::	445	::	0	2022.02.11.9:32:19	System
OneAppIGCC.WinServi...	2648	TCPv6	Listen	::	808	::	0	2022.02.11.9:32:21	igccservice
svchost.exe	14508	TCPv6	Listen	::	7680	::	0	2022.02.16.13:30:40	DoSvc
lsass.exe	924	TCPv6	Listen	::	49664	::	0	2022.02.11.9:32:18	lsass.exe
wininit.exe	824	TCPv6	Listen	::	49665	::	0	2022.02.11.9:32:18	wininit.exe
svchost.exe	1644	TCPv6	Listen	::	49666	::	0	2022.02.11.9:32:18	EventLog
svchost.exe	2188	TCPv6	Listen	::	49667	::	0	2022.02.11.9:32:18	Schedule
spoolsv.exe	3800	TCPv6	Listen	::	49668	::	0	2022.02.11.9:32:19	Spooler
jhi_service.exe	4692	TCPv6	Listen	::	49669	::	0	2022.02.11.9:32:19	jhi_service
services.exe	896	TCPv6	Listen	::	49670	::	0	2022.02.11.9:32:22	services.exe
chrome.exe	6492	TCPv6	Established	2001:738:6001:518:20e:744...	57016	2a00:1450:4025:402:bc...	5228	2022.02.16.15:00:50	chrome.exe
SearchApp.exe	16074	TCPv6	Close Wait	2001:738:6001:518:20e:744...	57404	2a01:1114:1004:001:4635...	443	2022.02.16.14:30:01	SearchApp.exe

Endpoints: 96 Established: 11 Listening: 32 Time Wait: Close Wait: 2 Update: 2 sec States: (All)

Egy program, amely megmutatja a rendszer összes TCP és UDP végpontjának részletes listáját, beleértve a helyi és távoli címeket és a TCP kapcsolatok állapotát

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

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-OK08NMS\Acer]

File Options View Process Find Users Help

Process CPU Private Bytes Working Set PID Description Company Name

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Susp...	184 K	40 344 K	72		
Registry		12 052 K	52 920 K	132		
System Idle Process	79.65	60 K	8 K	0		
System	0.36	196 K	96 K	4		
Interrupts	0.91	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 084 K	996 K	448		
Memory Compression	< 0.01	996 K	244 296 K	2556		
csrss.exe	< 0.01	2 104 K	4 372 K	724		
wininit.exe		1 832 K	5 184 K	824		
services.exe	0.18	6 776 K	10 308 K	896		
svchost.exe	0.36	19 560 K	32 136 K	3472	476 Windows-szolgáltatások gaz...	Microsoft Corporation
WmPrvSE.exe		6 708 K	9 656 K	3472		
WmPrvSE.exe		13 516 K	20 412 K	5324		
dllhost.exe		4 388 K				
ModJoCoreWorker.exe		38 120 K				
EapHost.exe		2 224 K				
SettingSyncHost.exe		2 376 K				
unsecapp.exe		1 452 K				
StartMenuExperienceHost.exe		23 508 K				
RuntimeBroker.exe		5 720 K				
SearchApp.exe	Susp...	88 612 K				
YourPhone.exe	Susp...	34 004 K				
RuntimeBroker.exe	Susp...	14 508 K				
RuntimeBroker.exe	Susp...	4 768 K				
RuntimeBroker.exe	Susp...	4 268 K				
IGCC.exe		22 164 K				
ApplicationFrameHost.exe		19 540 K				
Calculator.exe		21 788 K				
RuntimeBroker.exe		1 588 K				

CPU Usage: 17.05% Commit Charge: 54.03% Processes: 22

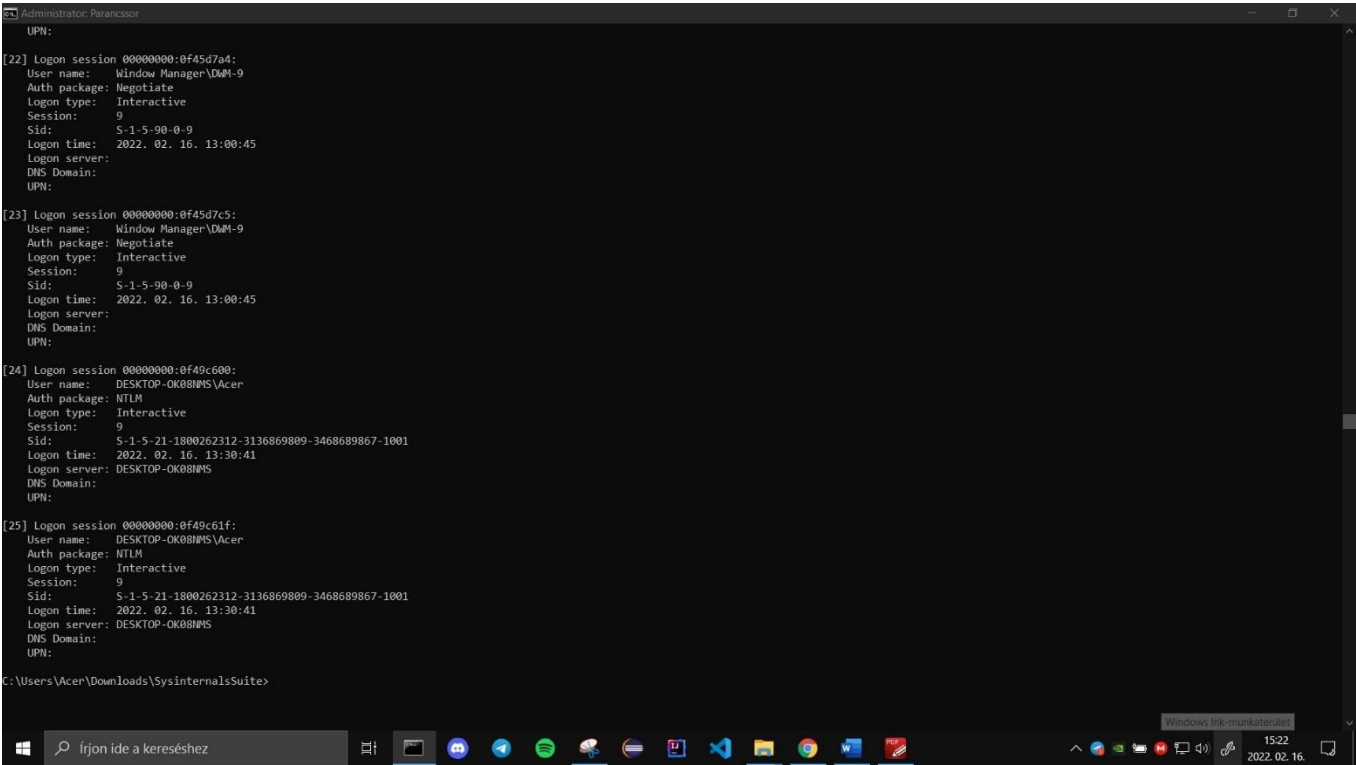
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
15:08:41	lsass.exe	924	QueryNameInfo	C:\Users\Acer\Downloads\Sysinternals...	SUCCESS	Name: (Users\Acer...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
15:08:41	Explorer.EXE	12556	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
15:08:41	Explorer.EXE	12556				

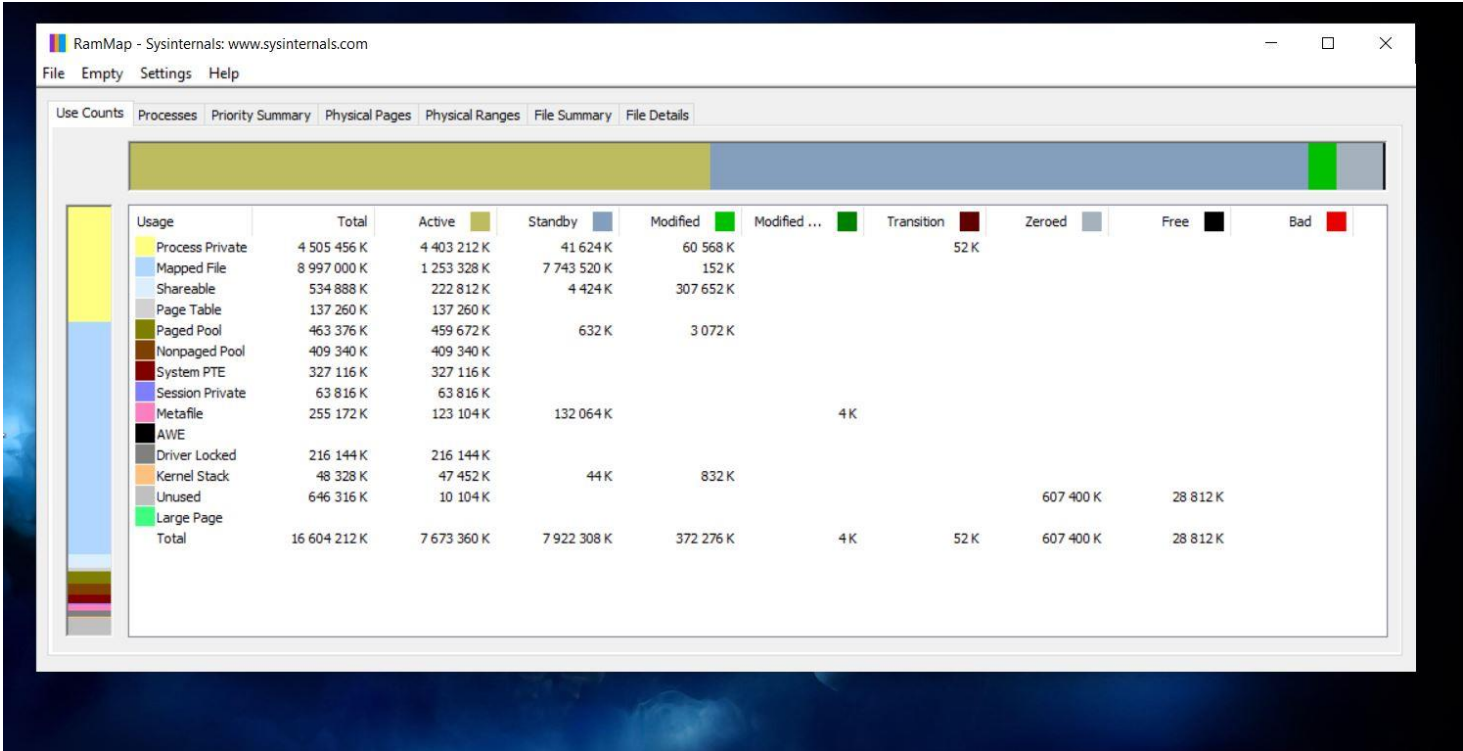


d) Security Utilities (LogonSession)



A program jegyzi a felhasználók bejelentkezését.

e) Information Utilities (RAMMap)



A program feladata a memória felhasználás monitorozása

### 3. Töltse le a következő programot: Dependency Walker

URL: <http://www.dependencywalker.com/>

*Feladata:* a segédprogram *megvizsgálja* milyen mappákra, és azon belül milyen függvényekre hivatkozik egy elindított program. „

Készítsen egy *neptunkod.c* nevű forráskódot, amely egy *vezeteknev.txt* fájlt létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc.

Fordítsa le kódot a C fordító, majd tegye futtathatóvá az állományt: *neptunkod.exe* A Dependency Walker segítségével végezze el a következő feladatokat.

Nyissa meg a *neptunkod.exe* fájlt!

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

Dependency Walker - [h2z4x3]

File Edit View Options Profile Window Help

H2Z4X3.EXE

- 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-CORE-PROCESSTHREADS-L1-1-0.DLL
  - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-3.DLL
  - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-2.DLL
  - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
  - API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL
  - API-MS-WIN-CORE-HEAP-L1-1-0.DLL
  - API-MS-WIN-CORE-HEAP-L2-1-0.DLL
  - API-MS-WIN-CORE-MEMORY-L1-1-1.DLL
  - API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
  - API-MS-WIN-CORE-MEMORY-L1-1-2.DLL
  - API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
  - API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
  - API-MS-WIN-CORE-SYNCH-L1-2-1.DLL
  - API-MS-WIN-CORE-SYNCH-L1-2-0.DLL
  - API-MS-WIN-CORE-FILE-L1-1-0.DLL
  - API-MS-WIN-CORE-FILE-L1-2-0.DLL
  - API-MS-WIN-CORE-FILE-L1-2-2.DLL

PI	Ordinal ^	Hint	Function	Entry Point
✓	N/A	269 (0x010D)	DeleteCriticalSection	Not Bound
✓	N/A	305 (0x0131)	EnterCriticalSection	Not Bound
✓	N/A	536 (0x0218)	GetCurrentProcess	Not Bound
✓	N/A	537 (0x0219)	GetCurrentProcessId	Not Bound
✓	N/A	541 (0x021D)	GetCurrentThreadId	Not Bound
✓	N/A	610 (0x0262)	GetLastError	Not Bound
✓	N/A	722 (0x02D2)	GetStartupInfoA	Not Bound
✓	N/A	747 (0x02EB)	GetSystemTimeAsFileTime	Not Bound
✓	N/A	775 (0x0307)	GetTickCount	Not Bound
✓	N/A	864 (0x0360)	InitializeCriticalSection	Not Bound
✓	N/A	952 (0x03B8)	LeaveCriticalSection	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
✓	1 (0x0001)	68 (0x0044)	BaseThreadInitThunk	0x0001FA10
✓	2 (0x0002)	883 (0x0373)	InterlockedPushListSList	NTDLL.RtlInterlockedPushListSList 0x00082034
✓	3 (0x0003)	1547 (0x0608)	Wow64Transition	NTDLL.RtlAcquireSRWLockExclusive
✓	4 (0x0004)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockShared
✓	5 (0x0005)	1 (0x0001)	AcquireSRWLockShared	0x00020AC0
✓	6 (0x0006)	2 (0x0002)	ActivateActCtx	0x00020400
✓	7 (0x0007)	3 (0x0003)	ActivateActCtxWorker	0x000195A0
✓	8 (0x0008)	4 (0x0004)	AddAtomA	0x0001B8D0
✓	9 (0x0009)	5 (0x0005)	AddAtomW	0x00023C10
✓	10 (0x000A)	6 (0x0006)	AddConsoleAliasA	

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. A rendszér nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszér nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. A rendszér nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. A rendszér nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. A rendszér nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. A rendszér nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL	Error opening file. A rendszér nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L2-2-2.DLL	Error opening file. A rendszér nem találja a megadott fájlt (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.  
Error: A circular dependency was detected.  
Warning: At least one delay-load dependency module was not found.  
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1

Dependency Walker - [h2z4x3]

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

Dependency Walker - [h2z4x3]

File Edit View Options Profile Window Help

h2z4x3.exe

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-CORE-PROCESSTHREADS-L1-1-0.DLL

API-MS-WIN-CORE-PROCESSTHREADS-L1-1-2.DLL

API-MS-WIN-CORE-PROCESSTHREADS-L1-1-3.DLL

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

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

API-MS-WIN-CORE-HEAP-L2-1-0.DLL

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

API-MS-WIN-CORE-MEMORY-L1-1-2.DLL

API-MS-WIN-CORE-MEMORY-L1-1-3.DLL

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

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

API-MS-WIN-CORE-SYNCH-L1-2-1.DLL

API-MS-WIN-CORE-SYNCH-L1-2-2.DLL

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

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

API-MS-WIN-CORE-FILE-L1-2-2.DLL

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	18 (0x0012)	ApiSetQueryApiSetPresence	Not Bound
	N/A	20 (0x0014)	CsrAllocateCaptureBuffer	Not Bound
	N/A	21 (0x0015)	CsrAllocateMessagePointer	Not Bound
	N/A	26 (0x001A)	CsrClientCallServer	Not Bound
	N/A	28 (0x001C)	CsrFreeCaptureBuffer	Not Bound
	N/A	32 (0x0020)	CsrVerifyRegion	Not Bound
	N/A	34 (0x0022)	DbgPrint	Not Bound
	N/A	35 (0x0023)	DbgPrintEx	Not Bound
	N/A	45 (0x002D)	DbgUiGetThreadDebugObject	Not Bound
	N/A	46 (0x002E)	DbgUiIssueRemoteBreakin	Not Bound
	N/A	57 (0x0039)	EtwEventEnabled	Not Bound
	N/A	59 (0x003B)	EtwEventRegister	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
	8 (0x0008)	918 (0x0396)	RtlDispatchAPC	0x0002C020
	9 (0x0009)	711 (0x02C7)	RtlActivateActivationContextUnsafeFast	0x0004DC60
	10 (0x000A)	876 (0x036C)	RtlDeactivateActivationContextUnsafeFast	0x0004C720
	11 (0x000B)	1167 (0x048F)	RtlInterlockedPushListSList	0x000BE9E0
	12 (0x000C)	1509 (0x05E5)	RtlUlongByteSwap	0x000BEA80
	13 (0x000D)	1510 (0x05E6)	RtlUlonglongByteSwap	0x000BEA90
	14 (0x000E)	1554 (0x0612)	RtlUshortByteSwap	0x000BEAB0
	15 (0x000F)	0 (0x0000)	A_SHAFinal	0x00067B30
	16 (0x0010)	1 (0x0001)	A_SHAInit	0x00088B80
	17 (0x0011)	2 (0x0002)	A_SHAUpdate	0x00067C10
	18 (0x0012)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount	0x000BEAC0

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L2-2-2.DLL	Error opening file. A rendszer nem találja a megadott fájlt (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.  
Error: A circular dependency was detected.  
Warning: At least one delay-load dependency module was not found.  
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1

Feladatkezelő

16:44  
2022.02.16.

Az ntdll.dll egy speciális, dinamikusan kapcsolódó könyvtár (Dynamically Linked Library) A Windows NT alapú operációs rendszerekben az ntdll.dll az user mód és a kernel mód közötti kommunikáció lebonyolításához