

# **Operációs rendszerek BSc**

2. Gyak.

2022. 02. 15.

**Készítette:**

Siska Dávid Bsc

Gazdaságinformatika

PJ8HD2

**Miskolc, 2022**

## 1. Készítse el a következő feladatokat!

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

### a.) Hozza létre a következő mappa szerkezetet!

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1526]
(c) Microsoft Corporation. Minden jog fenntartva.

C:\Users\siskad>D:
D:\>cd Letöltések
D:\Letöltések>cd Egyetem
D:\Letöltések\Egyetem>cd Oprendszerek
D:\Letöltések\Egyetem\Oprendszerek>mkdir PJ8HD2_0215
D:\Letöltések\Egyetem\Oprendszerek>cd PJ8HD2_0215
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215>mkdir pj8hd2
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215>cd pj8hd2
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>mkdir bokor
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>cd bokor
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor>mkdir banan
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor>mkdir mogyoro
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor>mkdir barack
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor>cd..
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>mkdir fa
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>cd fa
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa>mkdir korte
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa>cd..
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>mkdir land
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>cd land
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\land>mkdir szeder
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\land>mkdir kokusz
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\land>
```

### b.) Készítsen másolatot:

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

```
D:\pj8hd2>xcopy D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\land\szeder D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa /e
0 File(s) copied

D:\pj8hd2>
```

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

```
C:\Users\siskad>xcopy D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\banan D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa /e
0 File(s) copied

C:\Users\siskad>
```

### c.) Végezze el a következő áthelyezéseket:

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

```
D:\pj8hd2\land>move D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\barack D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa
1 dir(s) moved.

D:\pj8hd2\land>
```

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

```
D:\pj8hd2\land>move D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\land\kokusz D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa
1 dir(s) moved.

D:\pj8hd2\land>
```

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

állományokat:

```
D:\pj8hd2\land>rmdir D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\land /s
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\land, Are you sure (Y/N)? y

D:\pj8hd2\land>
```

neptunkod/bokor/banan/ leiras.txt

```
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\banan>type nul > leiras.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\banan>
```

neptunkod/tree/felsorolas.txt

```
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>type nul > felsorolas.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>
```

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

```
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\banan>echo "A barack egy sarga szinu gyumolcs">>leiras.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\banan>echo A barack egy sarga szinu gyumolcs > leiras.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\banan>echo A baracknak ket nagy fajtaja a sargabarack es az oszibarack>> leiras.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\banan>echo A barackot magrol ultetik>> leiras.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\banan>
```

A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

```
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>echo David >>felsorolas.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>echo Bence >>felsorolas.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>echo Mate >>felsorolas.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>echo Mark >>felsorolas.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>echo Kinga >>felsorolas.txt
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>
```

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

```
D: .
├── bokor
│   ├── banan
│   │   └── leiras.txt
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
└── tree
    └── felsorolas.txt

D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>
```

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

```
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>dir /s ?e*.txt
Volume in drive D is D  
Volume Serial Number is 1046-E311

Directory of D:\Letölt  sek\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\banan
2022. 02. 16. 17:31          124 leiras.txt
                1 File(s)          124 bytes

Directory of D:\Letölt  sek\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree
2022. 02. 16. 17:37          39 felsorolas.txt
                1 File(s)          39 bytes

Total Files Listed:
        2 File(s)          163 bytes
        0 Dir(s)  59 838 283 776 bytes free

D:\Letölt  sek\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>
```

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

```
D:\Letölt  sek\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>attrib -r "D:\Letölt  sek\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree\felsorolas.txt"
D:\Letölt  sek\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>
```

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

```
Parancssor
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>dir /s
Volume in drive D is D6
Volume Serial Number is 1046-E311

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2

2022. 02. 16. 17:08 <DIR>      .
2022. 02. 16. 17:08 <DIR>      ..
2022. 02. 16. 16:45 <DIR>      bokor
2022. 02. 16. 17:39 <DIR>      fa
2022. 02. 16. 17:08 <DIR>      tree
0 File(s)              0 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor

2022. 02. 16. 16:45 <DIR>      .
2022. 02. 16. 16:45 <DIR>      ..
2022. 02. 16. 17:06 <DIR>      banan
2022. 02. 15. 15:04 <DIR>      mogyoro
0 File(s)              0 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\banan

2022. 02. 16. 17:06 <DIR>      .
2022. 02. 16. 17:06 <DIR>      ..
2022. 02. 16. 17:31      124 leiras.txt
1 File(s)              124 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\bokor\mogyoro

2022. 02. 15. 15:04 <DIR>      .
2022. 02. 15. 15:04 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa

2022. 02. 16. 17:39 <DIR>      .
2022. 02. 16. 17:39 <DIR>      ..
2022. 02. 16. 17:39 <DIR>      banan
2022. 02. 15. 15:04 <DIR>      barack
2022. 02. 15. 15:05 <DIR>      kokusz
2022. 02. 15. 18:32 <DIR>      korte
2022. 02. 16. 17:39 <DIR>      szeder
0 File(s)              0 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa\banan

2022. 02. 16. 17:39 <DIR>      .
2022. 02. 16. 17:39 <DIR>      ..
0 File(s)              0 bytes
```

```
Parancssor
2022. 02. 15. 15:04 <DIR>      barack
2022. 02. 15. 15:05 <DIR>      kokusz
2022. 02. 15. 18:32 <DIR>      korte
2022. 02. 16. 17:39 <DIR>      szeder
0 File(s)              0 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa\banan

2022. 02. 16. 17:39 <DIR>      .
2022. 02. 16. 17:39 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa\barack

2022. 02. 15. 15:04 <DIR>      .
2022. 02. 15. 15:04 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa\kokusz

2022. 02. 15. 15:05 <DIR>      .
2022. 02. 15. 15:05 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa\korte

2022. 02. 15. 18:32 <DIR>      .
2022. 02. 15. 18:32 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\fa\szeder

2022. 02. 16. 17:39 <DIR>      .
2022. 02. 16. 17:39 <DIR>      ..
0 File(s)              0 bytes

Directory of D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree

2022. 02. 16. 17:08 <DIR>      .
2022. 02. 16. 17:08 <DIR>      ..
2022. 02. 16. 17:37      39 felsorolas.txt
1 File(s)              39 bytes

Total Files Listed:
2 File(s)              163 bytes
32 Dir(s) 59 838 251 088 bytes free

D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2>
```

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

```
D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>sort felsorolas.txt
Bence
David
Kinga
Mark
Mate

D:\Letöltések\Egyetem\Oprendszerek\PJ8HD2_0215\pj8hd2\tree>
```

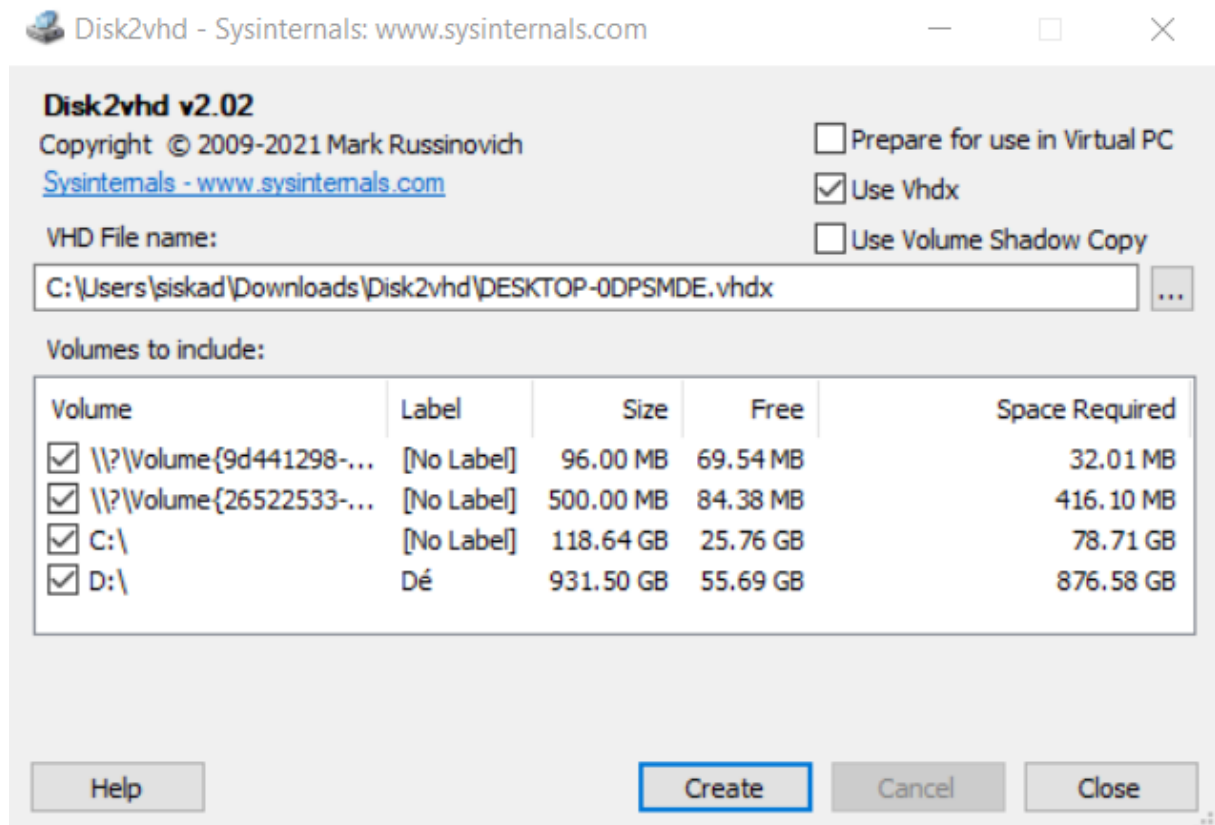
## 2. Feladat

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) File and Disk Utilities (Disk2vhd)



A Disk2vhd egy program, mely segítségével könnyedén készíthetünk merevlemezeinken tárolt fájlokról biztonsági mentést virtuális meghajtóként, tehát amelyet VHD-ként ment. Ezeket virtualbox-hoz és egyéb virtualizációs szoftverhez kapcsolhatunk.

## 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
svchost.exe	1100	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.12.21:21:31	RpcSs
System	4	TCP	Listen	192.168.0.109	139	0.0.0.0	0	2022.02.18.13:37:22	System
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.02.18.13:37:25	System
OneApp.IGCC.WinServi...	4428	TCP	Listen	0.0.0.0	808	0.0.0.0	0	2022.02.12.21:21:35	igccservice
Messenger.exe	10720	TCP	Listen	127.0.0.1	3103	0.0.0.0	0	2022.02.18.8:47:34	Messenger.exe
svchost.exe	6660	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.18.13:37:22	CDPSvc
SearchApp.exe	816	TCP	Close Wait	192.168.0.109	49435	92.122.242.18	443	2022.02.18.16:47:10	SearchApp.exe
SearchApp.exe	816	TCP	Close Wait	192.168.0.109	49438	91.83.14.136	443	2022.02.18.16:47:11	SearchApp.exe
SearchApp.exe	816	TCP	Close Wait	192.168.0.109	49441	91.83.14.136	443	2022.02.18.16:47:11	SearchApp.exe
Isass.exe	892	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.02.12.21:21:31	Isass.exe
wininit.exe	800	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.02.12.21:21:31	wininit.exe
svchost.exe	1540	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.02.12.21:21:32	EventLog
svchost.exe	1564	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022.02.12.21:21:32	Schedule
spoolsv.exe	4064	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2022.02.12.21:21:34	Spooler
services.exe	872	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	2022.02.12.21:21:38	services.exe
chrome.exe	10188	TCP	Established	192.168.0.109	50472	35.234.126.59	443	2022.02.18.16:58:17	chrome.exe
chrome.exe	10188	TCP	Established	192.168.0.109	50527	151.101.112.193	443	2022.02.18.17:05:56	chrome.exe
chrome.exe	10188	TCP	Established	192.168.0.109	50540	20.75.32.255	443	2022.02.18.17:05:58	chrome.exe
chrome.exe	10188	TCP	Established	192.168.0.109	50601	140.82.113.25	443	2022.02.18.17:10:58	chrome.exe
Messenger.exe	10720	TCP	Established	192.168.0.109	50614	185.60.218.35	443	2022.02.18.17:12:39	Messenger.exe
Messenger.exe	10720	TCP	Established	192.168.0.109	50615	185.60.218.35	443	2022.02.18.17:12:39	Messenger.exe
[Time Wait]		TCP	Time Wait	192.168.0.109	50617	142.250.180.238	443		
chrome.exe	10188	TCP	Established	192.168.0.109	50619	13.107.213.44	443	2022.02.18.17:12:57	chrome.exe

Endpoints: 142 Established: 37 Listening: 29 Time Wait: 12 Close Wait: 3 Update: 2 sec States: (All)

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.

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

### Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-0DPSMDE\siskad]

File Options View Process Find Users Help

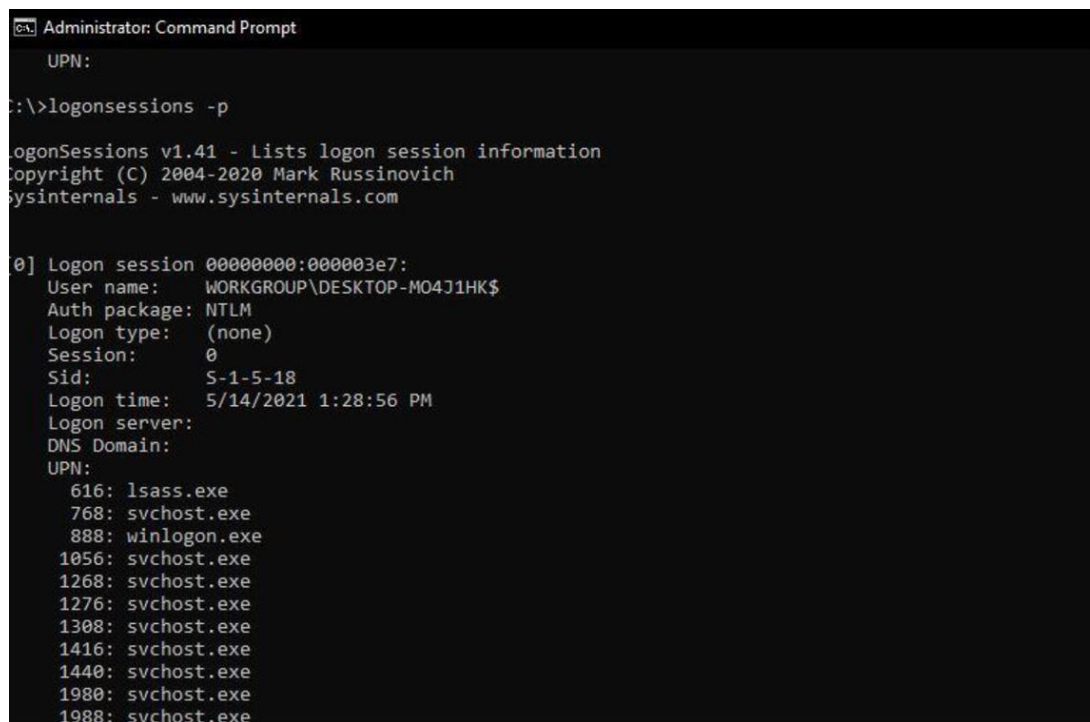
<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		9 344 K	50 892 K	108		
System Idle Process	92.54	60 K	8 K	0		
System	< 0.01	196 K	32 K	4		
Interrupts	1.11	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 060 K	492 K	424		
Memory Compression	< 0.01	2 188 K	303 844 K	8		
csrss.exe		1 900 K	2 676 K	696		
wininit.exe		1 616 K	3 024 K	800		
services.exe		6 940 K	10 648 K	872		
svchost.exe	< 0.01	18 184 K	28 000 K	664	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPrvSE.exe		3 156 K	7 428 K	3388		
MoUsCoreWorker.exe		39 160 K	46 808 K	12748		
SettingSyncHost.exe		2 428 K	5 172 K	9840	Host Process for Setting Syn...	Microsoft Corporation
StartMenuExperienceHo...		32 384 K	86 408 K	11652		
RuntimeBroker.exe		6 432 K	23 596 K	14148	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	128 176 K	105 540 K	592	Search application	Microsoft Corporation
RuntimeBroker.exe		17 396 K	43 772 K	13440	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	35 380 K	5 540 K	9952		Microsoft Corporation
RuntimeBroker.exe		6 772 K	25 012 K	3548	Runtime Broker	Microsoft Corporation
TextInputHost.exe		14 076 K	47 248 K	9464		Microsoft Corporation
RuntimeBroker.exe		3 292 K	20 996 K	11856	Runtime Broker	Microsoft Corporation
Cortana.exe		31 904 K	69 688 K	10612	Cortana	Microsoft Corporation
RuntimeBroker.exe		5 068 K	26 964 K	4828	Runtime Broker	Microsoft Corporation
Win32Bridge.Server.e...		9 024 K	24 744 K	10292	Cortana System Service	Microsoft Corporation
ApplicationFrameHoste...		14 328 K	34 732 K	4300	Application Frame Host	Microsoft Corporation
Video.UI.exe	Susp...	18 796 K	2 132 K	11760		
SystemSettings.exe	Susp...	26 152 K	2 660 K	6152	Gépház	Microsoft Corporation
UserOOBEBroker.exe		1 988 K	9 396 K	7664	User OOBEBroker	Microsoft Corporation
Calculator.exe	Susp...	22 508 K	2 216 K	13332		
RuntimeBroker.exe		1 596 K	6 492 K	2404	Runtime Broker	Microsoft Corporation

CPU Usage: 8.14% Commit Charge: 71.13% Processes: 242 Physical Usage: 78.54%

A Process Explorer használatával a számítógépen futó folyamatokról hierarchikus fa nézet jelenik meg, beleértve a CPU és a RAM használatát az egyes folyamatok számértékeivel.

#### d) Security Utilities (LogonSession)



```
Administrator: Command Prompt

UPN:

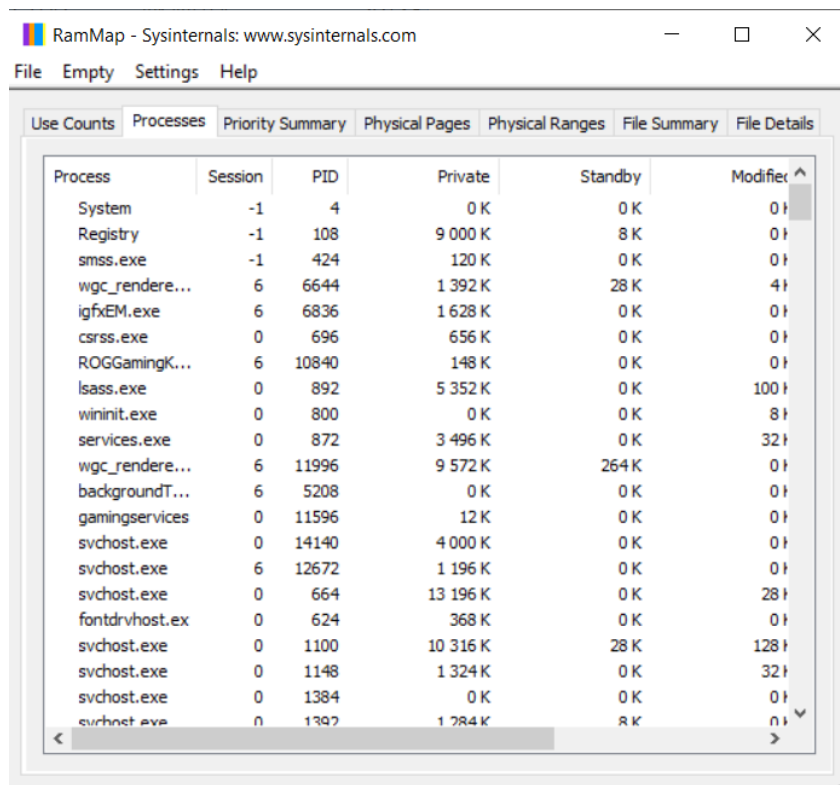
C:\>logonsessions -p

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

[0] Logon session 00000000:000003e7:
User name:      WORKGROUP\DESKTOP-M04J1HK$
Auth package:   NTLM
Logon type:      (none)
Session:         0
Sid:             S-1-5-18
Logon time:      5/14/2021 1:28:56 PM
Logon server:
DNS Domain:
UPN:
  616: lsass.exe
  768: svchost.exe
  888: winlogon.exe
 1056: svchost.exe
 1268: svchost.exe
 1276: svchost.exe
 1308: svchost.exe
 1416: svchost.exe
 1440: svchost.exe
 1980: svchost.exe
 1988: svchost.exe
```

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

#### e) Information Utilities (RAMMap)



Process	Session	PID	Private	Standby	Modifier
System	-1	4	0 K	0 K	0↑
Registry	-1	108	9 000 K	8 K	0↑
smss.exe	-1	424	120 K	0 K	0↑
wgc_rendere...	6	6644	1 392 K	28 K	4↑
igfxEM.exe	6	6836	1 628 K	0 K	0↑
csrss.exe	0	696	656 K	0 K	0↑
ROGGamingK...	6	10840	148 K	0 K	0↑
lsass.exe	0	892	5 352 K	0 K	100↑
wininit.exe	0	800	0 K	0 K	8↑
services.exe	0	872	3 496 K	0 K	32↑
wgc_rendere...	6	11996	9 572 K	264 K	0↑
backgroundT...	6	5208	0 K	0 K	0↑
gamingservices	0	11596	12 K	0 K	0↑
svchost.exe	0	14140	4 000 K	0 K	0↑
svchost.exe	6	12672	1 196 K	0 K	0↑
svchost.exe	0	664	13 196 K	0 K	28↑
fontdrvhost.ex	0	624	368 K	0 K	0↑
svchost.exe	0	1100	10 316 K	28 K	128↑
svchost.exe	0	1148	1 324 K	0 K	32↑
svchost.exe	0	1384	0 K	0 K	0↑
svchost.exe	0	1392	1 284 K	8 K	0↑



RAMMap segítségével pontosan felderíthetővé válik, hogy a Windows pontosan milyen komponenseknek és mennyi memóriát foglal le.

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).

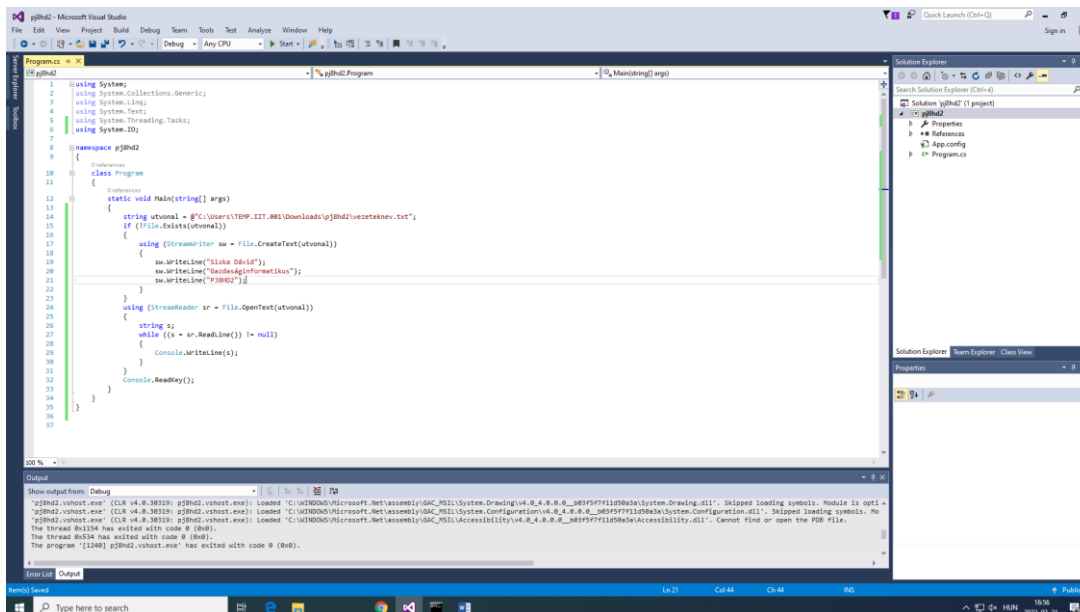
### 3. Feladat

Tölts 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 - [pj3hd2]

File Edit View Options Profile Window Help

Pj3hd2.EXE

- MSCORE.DLL
  - API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
    - NTDLL.DLL
      - KERNELBASE.DLL
        - API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
          - API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
            - API-MS-WIN-CORE-APIQUERY-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-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

| PI | Ordinal ^    | Hint | Function                 | Entry Point |
|----|--------------|------|--------------------------|-------------|
|    | 0 (0x0000)   |      | AcquireSRWLockExclusive  | Not Bound   |
|    | 57 (0x0039)  |      | CloseHandle              | Not Bound   |
|    | 103 (0x0067) |      | CreateEventW             | Not Bound   |
|    | 112 (0x0070) |      | CreateFileMappingW       | Not Bound   |
|    | 115 (0x0073) |      | CreateFileW              | Not Bound   |
|    | 128 (0x0080) |      | CreateMutexW             | Not Bound   |
|    | 142 (0x008E) |      | CreateSemaphoreW         | Not Bound   |
|    | 156 (0x009C) |      | CreateToolhelp32Snapshot | Not Bound   |
|    | 166 (0x00A6) |      | DebugBreak               | Not Bound   |

| E | Ordinal ^  | Hint       | Function                | Entry Point                      |
|---|------------|------------|-------------------------|----------------------------------|
|   | 1 (0x0001) | 0 (0x0000) | AcquireSRWLockExclusive | NTDLL.RtlAcquireSRWLockExclusive |
|   | 2 (0x0002) | 1 (0x0001) | AcquireSRWLockShared    | NTDLL.RtlAcquireSRWLockShared    |
|   | 3 (0x0003) | 2 (0x0002) | ActivateActCtx          | 0x0001E690                       |
|   | 4 (0x0004) | 3 (0x0003) | ActivateActCtxWorker    | 0x0001A9A0                       |
|   | 5 (0x0005) | 4 (0x0004) | AddAtomA                | 0x000216A0                       |
|   | 6 (0x0006) | 5 (0x0005) | AddAtomW                | 0x00010890                       |
|   | 7 (0x0007) | 6 (0x0006) | AddConsoleAliasA        | 0x000228C0                       |
|   | 8 (0x0008) | 7 (0x0007) | AddConsoleAliasW        | 0x000228D0                       |

| Module                | File Time Stamp  | Link Time Stamp  | File Size | Attr. | Link Checksum | Real Checksum | CPU | Subsystem | Symbols    | Preferred Base ^   | Actual ^ |
|-----------------------|------------------|------------------|-----------|-------|---------------|---------------|-----|-----------|------------|--------------------|----------|
| COML2.DLL             | 2019/03/19 5:44  | 2036/05/10 6:19  | 477 240   | A     | 0x0007F706    | 0x0007F706    | x64 | Console   | CV,Unknown | 0x0000000180000000 | Unkno    |
| CONTACTACTIVATION.DLL | 2019/03/19 5:44  | 2056/11/21 19:01 | 56 320    | A     | 0x0001130E    | 0x0001130E    | x64 | Console   | CV,Unknown | 0x0000000180000000 | Unkno    |
| COREMESSAGING.DLL     | 2021/12/14 12:18 | 2051/05/09 1:05  | 858 928   | A     | 0x000D47C6    | 0x000D47C6    | x64 | GUI       | CV,Unknown | 0x0000000180000000 | Unkno    |
| COREUICOMPONENTS.DLL  | 2021/12/14 12:17 | 2052/10/27 12:25 | 3 327 776 | A     | 0x0032F133    | 0x0032F133    | x64 | GUI       | CV,Unknown | 0x0000000180000000 | Unkno    |
| CREDUI.DLL            | 2019/03/19 5:44  | 1992/11/03 3:34  | 49 152    | A     | 0x00018F42    | 0x00018F42    | x64 | Console   | CV,Unknown | 0x0000000180000000 | Unkno    |
| CRYPT32.DLL           | 2021/12/14 12:18 | 1977/06/25 15:25 | 1 330 952 | A     | 0x00152CFE    | 0x00152CFE    | x64 | GUI       | CV,Unknown | 0x0000000180000000 | Unkno    |
| CRYPTBASE.DLL         | 2019/03/19 5:44  | 2105/07/16 1:07  | 33 848    | A     | 0x0000FC85    | 0x0000FC85    | x64 | Console   | CV,Unknown | 0x0000000180000000 | Unkno    |
| CRYPTNET.DLL          | 2019/03/19 5:44  | 2065/05/12 11:08 | 168 448   | A     | 0x0002B098    | 0x0002B098    | x64 | GUI       | CV,Unknown | 0x0000000180000000 | Unkno    |

Error: At least one required implicit or forwarded dependency was not found.  
 Error: Modules with different CPU types were found.  
 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

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

Dependency Walker - [pj3hd2]

File Edit View Options Profile Window Help

Pj3hd2.EXE

- MSCORE.DLL
  - API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
    - NTDLL.DLL
      - KERNELBASE.DLL
        - API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
          - API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
            - API-MS-WIN-CORE-APIQUERY-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-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

| PI | Ordinal ^  | Hint        | Function                                    | Entry Point |
|----|------------|-------------|---|-------------|
|    | 8 (0x0008) |             | N/A   | Not Bound   |
|    | N/A        | 20 (0x0014) | CsrAllocateCaptureBuffer                    | Not Bound   |
|    | N/A        | 21 (0x0015) | CsrAllocateMessagePointer                   | Not Bound   |
|    | N/A        | 22 (0x0016) | CsrCaptureMessageBuffer                     | Not Bound   |
|    | N/A        | 23 (0x0017) | CsrCaptureMessageMultiUnicodeStringsInPlace | Not Bound   |
|    | N/A        | 26 (0x001A) | CsrClientCallServer                         | Not Bound   |
|    | N/A        | 27 (0x001B) | CsrClientConnectToServer                    | Not Bound   |
|    | N/A        | 28 (0x001C) | CsrFreeCaptureBuffer                        | Not Bound   |
|    | N/A        | 29 (0x001D) | CsrGetProcessId                             | Not Bound   |

| E | Ordinal ^   | Hint       | Function                                    | Entry Point |
|---|-------------|------------|---|-------------|
|   | 8 (0x0008)  | N/A        | N/A   | 0x0007CF40  |
|   | 9 (0x0009)  | 0 (0x0000) | A_SHAFinal                                  | 0x0000C4D0  |
|   | 10 (0x000A) | 1 (0x0001) | A_SHAInit                                   | 0x0000C600  |
|   | 11 (0x000B) | 2 (0x0002) | A_SHAUpdate                                 | 0x0000C640  |
|   | 12 (0x000C) | 3 (0x0003) | AlpcAdjustCompletionListConcurrencyCount    | 0x000DF A30 |
|   | 13 (0x000D) | 4 (0x0004) | AlpcFreeCompletionListMessage               | 0x0006C550  |
|   | 14 (0x000E) | 5 (0x0005) | AlpcGetCompletionListLastMessageInformation | 0x000DF A60 |
|   | 15 (0x000F) | 6 (0x0006) | AlpcGetCompletionListMessageAttributes      | 0x000DF A80 |

| Module                | File Time Stamp  | Link Time Stamp  | File Size | Attr. | Link Checksum | Real Checksum | CPU | Subsystem | Symbols    | Preferred Base ^   | Actual ^ |
|-----------------------|------------------|------------------|-----------|-------|---------------|---------------|-----|-----------|------------|--------------------|----------|
| COML2.DLL             | 2019/03/19 5:44  | 2036/05/10 6:19  | 477 240   | A     | 0x0007F706    | 0x0007F706    | x64 | Console   | CV,Unknown | 0x0000000180000000 | Unkno    |
| CONTACTACTIVATION.DLL | 2019/03/19 5:44  | 2056/11/21 19:01 | 56 320    | A     | 0x0001130E    | 0x0001130E    | x64 | Console   | CV,Unknown | 0x0000000180000000 | Unkno    |
| COREMESSAGING.DLL     | 2021/12/14 12:18 | 2051/05/09 1:05  | 858 928   | A     | 0x000D47C6    | 0x000D47C6    | x64 | GUI       | CV,Unknown | 0x0000000180000000 | Unkno    |
| COREUICOMPONENTS.DLL  | 2021/12/14 12:17 | 2052/10/27 12:25 | 3 327 776 | A     | 0x0032F133    | 0x0032F133    | x64 | GUI       | CV,Unknown | 0x0000000180000000 | Unkno    |
| CREDUI.DLL            | 2019/03/19 5:44  | 1992/11/03 3:34  | 49 152    | A     | 0x00018F42    | 0x00018F42    | x64 | Console   | CV,Unknown | 0x0000000180000000 | Unkno    |
| CRYPT32.DLL           | 2021/12/14 12:18 | 1977/06/25 15:25 | 1 330 952 | A     | 0x00152CFE    | 0x00152CFE    | x64 | GUI       | CV,Unknown | 0x0000000180000000 | Unkno    |
| CRYPTBASE.DLL         | 2019/03/19 5:44  | 2105/07/16 1:07  | 33 848    | A     | 0x0000FC85    | 0x0000FC85    | x64 | Console   | CV,Unknown | 0x0000000180000000 | Unkno    |
| CRYPTNET.DLL          | 2019/03/19 5:44  | 2065/05/12 11:08 | 168 448   | A     | 0x0002B098    | 0x0002B098    | x64 | GUI       | CV,Unknown | 0x0000000180000000 | Unkno    |

Error: At least one required implicit or forwarded dependency was not found.  
 Error: Modules with different CPU types were found.  
 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

Az ntdll.dll egy olyan modul, amely NT rendszerfunkciókat tartalmaz. Az ntdll.dll fájl a Microsoft által létrehozott fájl, amely az „NT Layer DLL” leírását tartalmazza, és amely NT kernelfunkciókat tartalmaz.

A c:\windows\system32 vagy c:\winnt\system32 könyvtárban található, illetve a c:\i386 könyvtárban is megtalálható.

Mentés: Írja le a program szolgáltatásait és a futtatás eredményét a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).